BayRS Version 14.10

Part No. 308624-14.10 Rev 01
January 2000

4401 Great America Parkway
Santa Clara, CA 95054

Configuring Frame Relay Services

NORTEL NETWORKS™

Copyright © 1999 Nortel Networks

All rights reserved. Printed in the USA. January 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks is a registered trademark and ASN, BayRS, BayStack, and BCC are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xvii
Text Conventions xviii
Acronyms xix
Hard-Copy Technical Manuals xxi
How to Get Help xxii

Chapter 1
Frame Relay Overview

Introduction to Frame Relay 1-2
Permanent Virtual Circuits 1-3
Switched Virtual Circuits 1-3
PVC and SVC Comparison 1-4
Frame Relay Packets 1-5
Management Protocols 1-7
Frame Relay SVC Signaling and LAPF 1-8
LAPF Operational States 1-9
LAPF Timeout and Retransmission Timers 1-10
Timer T200 1-10
Timer T203 1-11
SVC Signaling 1-11
Call Setup 1-11
Message Processing 1-13
Frame Relay Service Records 1-14
Default Service Record 1-14
Multiple Service Records 1-15
Adding and Moving PVCs 1-15
Frame Relay Access Modes 1-15
Group Access Mode 1-15

Direct Access Mode 1-16
Hybrid Access Mode 1-16
Using Hybrid Mode for Transparent Bridging 1-17
Source Routing 1-18
RFC 1490 1-18
Address Resolution for PVCs 1-18
Address Resolution for SVCs 1-19
Traffic Control 1-19
Data Compression 1-20
Data Encryption 1-21
Protocol Prioritization 1-21
Congestion Control 1-22
Traffic Shaping 1-23
Committed Information Rate 1-23
Committed Burst Rate and Excess Burst Rate 1-24
Quality of Service 1-25
Traffic Shaping for SVCs 1-27
Requesting Quality of Service 1-27
Refining Quality of Service 1-28
Traffic Shaping Configuration Notes for PVCs and SVCs 1-29
CIR Configuration Guidelines 1-29
Using Data Compression and Traffic Shaping 1-30
Oversubscribing the Traffic Shaping Interface 1-31
Queue Limits and Data Clipping 1-31
Congestion Counters and Timers 1-32
X.213 Priority for SVCs 1-33
Inactivity Timing for SVCs 1-33
Managing Routing Information Protocol (RIP) and Inactivity Timing 1-34
Multiline for PVCs 1-35
Traffic Distribution Between Data Paths 1-36
Random Distribution 1-36
Address-Based Distribution 1-37
Protocol Prioritization and Multiline Incompatibility 1-37
PVC Pass-Through 1-37
Frame Relay Dial Services 1-38

Synchronous Line Configuration for Frame Relay 1-38
Calculating the MTU Size for Frame Relay Connections 1-39

Chapter 2
Starting Frame Relay

Starting Configuration Tools 2-1
Preparing a Configuration File 2-2
Starting Frame Relay 2-2
Configuring PVCs and SVCs 2-4
Configuring a PVC 2-4
Configuring an SVC 2-6
Configuring Adjacent Hosts for an SVC Service Record 2-7

Chapter 3
Customizing Frame Relay Interfaces

Configuring Interfaces Using the BCC or Site Manager 3-1
Selecting a Management Type 3-2
Setting XOFF Control 3-4
Selecting Address Type and Length 3-5
Selecting a DLCI Address Type 3-5
Selecting a DLCI Address Length 3-5
Monitoring the Connection 3-7
Polling Interval 3-7
Full Enquiry Interval 3-8
Error Threshold and Monitored Events 3-8
Polling Interval 3-9
Full Enquiry Interval 3-9
Error Threshold 3-10
Monitored Events 3-10
Deleting Frame Relay 3-12

Chapter 4
Customizing PVCs

Configuring PVCs Using the BCC or Site Manager 4-2
Adding Service Records 4-3
Deleting Service Records 4-4
Adding PVCs to Service Records 4-5

Deleting PVCs from Service Records 4-7
Moving PVCs from One Service Record to Another 4-9
Enabling Multicast 4-10
Configuring Hybrid Mode for PVCs 4-12
Configuring PVC Pass-Through 4-13
Configuring Pass-Through PVCs 4-13
Mapping Pass-Through PVCs 4-14
Controlling Congestion for PVCs 4-15
Configuring Congestion Control for an Interface 4-15
Congestion Control 4-16
Congestion Timer 4-16
Congestion Counter 4-17
Congestion Method 4-17
Configuring Congestion Control for Individual PVCs 4-18
Congestion Control 4-19
Congestion Timer 4-19
Congestion Counter 4-20
Congestion Method 4-20
Using Traffic Shaping 4-21
Normal, High, and Low Queue Limits 4-22
Committed Burst 4-23
Excess Burst 4-23
CIR (Throughput) 4-24
Disabling and Reenabling Data Compression for PVCs 4-26
Grouping Service Records for Multiline Mode 4-27
Removing Multiline Services 4-28

Chapter 5
Customizing SVCs

Adding Service Records for SVCs 5-2
Deleting Service Records for SVCs 5-4
Call Screening and Blocking 5-5
SVC Call Block Direction 5-5
SVC Screening 5-6
SVC Screen Usage 5-6
Adding SVC Options to Service Records 5-7

Disabling SVCs 5-9
Disconnecting Active SVCs 5-10
Modifying LAPF Parameters for SVCs 5-11
State 5-12
Station Type 5-12
Initiation Mode 5-13
Retransmission Timer 5-13
Idle Timer 5-14
Retransmission Limit 5-14
Information Limit 5-15
Window Size 5-15
Modifying Signaling Parameters for SVCs 5-17
State 5-17
Maximum SVCs 5-18
Setup Timer 5-18
Disconnect Timer 5-19
Release Timer 5-19
Call Proceeding Timer 5-20
Status Enquiry Timer 5-20
Status Enquiry Retry 5-21
Setting Inactivity Values for SVCs 5-22
Service Record Inactivity Values 5-22
Individual SVC Inactivity Values 5-24
Controlling Congestion for SVCs 5-26
Configuring Congestion Control for an Interface 5-27
Congestion Control 5-27
Congestion Timer 5-27
Congestion Counter 5-28
Congestion Method 5-28
Configuring Congestion Control for Individual SVCs 5-30
Congestion Control 5-30
Congestion Timer 5-30
Congestion Counter 5-31
Congestion Method 5-31
Using Traffic Shaping with SVCs 5-33

Enabling Traffic Shaping 5-33
Customizing Traffic Shaping Quality of Service 5-35
Committed Burst 5-35
Excess Burst 5-36
CIR (Throughput) 5-37
Disabling and Reenabling Data Compression for SVCs 5-39
Setting X.213 Priorities for SVCs 5-41

Appendix A
Site Manager Parameters

Interface Parameters A-2
SVC LAPF Parameters A-12
SVC Signaling Parameters A-17
Service Name Parameter A-22
PVC Parameters A-24
DLCI Parameter for Each PVC A-24
PVC Service Record Parameters A-26
Multiline Algorithm Parameter A-32
C Service Record Parameters A-35
SVC Service List Parameters A-35
SVC Options Parameters A-41
SVC Options List for Service Parameters A-44

Appendix B
RIP Management for Frame Relay SVCs

Appendix C
Monitoring Frame Relay Using the BCC show Command

Online Help for show Commands C-2
show frame-relay congestion C-2
show frame-relay multiline C-4
show frame-relay services C-5
show frame-relay shaping C-6
show frame-relay stats C-7
show frame-relay stats dlcmi C-7
show frame-relay stats error C-8

show frame-relay stats lapf C-9
show frame-relay stats lapf errors C-9
show frame-relay stats lapf receive C-10
show frame-relay stats lapf traffic C-11
show frame-relay stats lapf transmit C-11
show frame-relay stats shaping C-12
show frame-relay stats signalling C-13
show frame-relay stats signalling receive C-14
show frame-relay stats signalling transmit C-15
show frame-relay stats vcs C-16
show frame-relay summary C-17
show frame-relay svcs C-19
show frame-relay svcs calls C-19
show frame-relay svcs priority C-20
show frame-relay svcs shaping C-20
show frame-relay vcs C-21

Index

Figures

Figure 1-1. Frame Relay Network 1-2
Figure 1-2. Frame Relay Header: 2-Byte Format 1-6
Figure 1-3. Frame Relay Header: 3- and 4-Byte Formats 1-6
Figure 1-4. Structure of the DLCMI 1-7
Figure 1-5. Frame Relay Signaling and LAPF Standards 1-8
Figure 1-6. Hybrid Mode Configuration, Non-Fully Meshed Network 1-16
Figure 1-7. Example of a Bridged Network 1-17
Figure 1-8. Big Pipe/Little Pipe Topology 1-20
Figure 1-9. Detecting and Controlling Network Congestion 1-22
Figure 1-10. Traffic Shaping Queues 1-26
Figure 1-11. FECNs and BECNs in Big Pipe/Little Pipe Topology 1-33
Figure 1-12. Multiline Network 1-35
Figure 1-13. PVC Pass-Through 1-38
Figure A-1. Frame Relay Interface List Window (for PVCs) A-2
Figure A-2. Frame Relay Interface List Window (for SVCs) A-3
Figure A-3. FR LAPF Parameters Window A-12
Figure A-4. Frame Relay Signaling Parameters Window A-17
Figure A-5. Frame Relay Service List Window (for PVCs) A-22
Figure A-6. Frame Relay PVC Add Window A-24
Figure A-7. FR PVC List for Service Window A-26
Figure A-8. Services Multilined With Window A-32
Figure A-9. Add Multiline Services Window A-33
Figure A-10. Frame Relay Service List Window (for SVCs) A-35
Figure A-11. Frame Relay SVC Options Add Window A-41
Figure A-12. FR SVC Options List for Service Window A-44

Tables

Table 1-1. PVC and SVC Protocol and Feature Support 1-4
Table 1-2. LAPF Timeout and Retransmission Timers 1-10
Table 1-3. Network Timers 1-12
Table 1-4. Message Processing 1-13
Table 1-5. How Protocols Handle Address Resolution 1-19
Table 1-6. Incoming and Outgoing 1-29
Table 1-7. Inactivity Timer and Inactivity Timer Mode Interaction 1-34
Table 1-8. Synchronous Line Parameters for Frame Relay 1-39
Table 1-9. MTU Adjustments for Frame Relay Connections 1-40
Table 3-1. Interface Configuration Tasks 3-1
Table 4-1. PVC Configuration Tasks 4-2
Table B-1. RIP Parameters B-2

Preface

This guide describes frame relay and what you do to start and customize frame relay services on a Nortel Networks™ router.

You can use the Bay Command Console (BCC™) or Site Manager to configure frame relay on a router. In this guide, you will find instructions for using both the BCC and Site Manager.

Before You Begin

Before using this guide with a new router, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.
- Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [<*parameter*> <*value*>] **. . .** , you enter **ethernet/2/1** and as many parameter-value pairs as needed.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.

`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B_c	committed burst rate
B_e	excess burst
BCC	Bay Command Console
BECN	backward explicit congestion notification
BofL	Breath of Life (message)
C/R	command/response bit
CIR	committed information rate
CRC	cyclic redundancy check
DCE	data communications equipment
DE	discard eligibility
DLCI	data link connection identifier

DLCMI	Data Link Control Management Interface
DTE	data terminal equipment
EA	extended address bit
FECN	forward explicit congestion notification
FRAD	frame relay access devices
FTP	File Transfer Protocol
HSSI	High-Speed Serial Interface
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunication Union–Telecommunications sector (formerly CCITT)
LAN	local area network
LAPF	link access procedure, frame mode
LMI	Local Management Interface
MAC	media access control
MIB	management information base
MTU	maximum transmission unit
OSI	Open Systems Interconnection
PRI	Primary Rate Interface
PVC	permanent virtual circuit
QoS	quality of service
SABME	set asynchronous balanced mode extended
SNA	Systems Network Architecture
SVC	switched virtual circuit
T_c	time interval
TEI	terminal endpoint identifier
TelNet	Telecommunications Network
TFTP	Trivial File Transfer Protocol

UA	unnumbered acknowledgment
URL	uniform resource locator
VC	virtual circuit
WAN	wide area network
WCP	WAN Compression Protocol
WEP	WAN Encryption Protocol
XNS	Xerox Networking System

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase selected documentation sets, CDs, and technical publications through the collateral catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Chapter 1
Frame Relay Overview

The following sections present an overview of frame relay.

Topic	Page
Introduction to Frame Relay	1-2
Permanent Virtual Circuits	1-3
Switched Virtual Circuits	1-4
PVC and SVC Comparison	1-4
Frame Relay Packets	1-5
Management Protocols	1-7
Frame Relay SVC Signaling and LAPF	1-8
SVC Signaling	1-11
Frame Relay Service Records	1-14
Frame Relay Access Modes	1-15
Source Routing	1-18
RFC 1490	1-18
Address Resolution for PVCs	1-18
Address Resolution for SVCs	1-19
Traffic Control	1-19
Data Compression	1-20
Data Encryption	1-21
Protocol Prioritization	1-21
Congestion Control	1-22
Traffic Shaping	1-23

(continued)

Topic *(continued)*	**Page**
Traffic Shaping for SVCs	1-27
Traffic Shaping Configuration Notes for PVCs and SVCs	1-29
X.213 Priority for SVCs	1-33
Inactivity Timing for SVCs	1-33
Multiline for PVCs	1-35
PVC Pass-Through	1-37
Frame Relay Dial Services	1-38
Synchronous Line Configuration for Frame Relay	1-38
Calculating the MTU Size for Frame Relay Connections	1-39

Introduction to Frame Relay

Frame relay is a high-speed, packet-switching WAN protocol that connects geographically dispersed LANs. Frame relay is usually offered by a public network provider; however, private organizations can acquire and manage their own frame relay networks as well.

Frame relay is a connection-oriented protocol, which means that it relies on end-to-end paths between devices connected across the network. It implements these connections using permanent virtual circuits or switched virtual circuits.

Figure 1-1 illustrates a frame relay network.

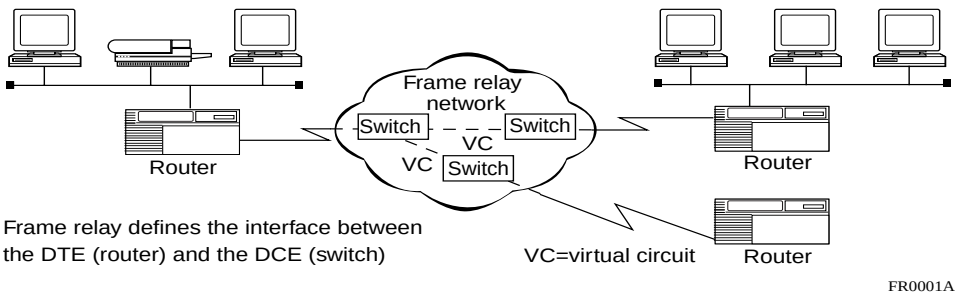

Figure 1-1. Frame Relay Network

Frame relay assumes that networks use transmission lines with low error rates, such as digital transmission media. Consequently, frame relay provides only basic error detection with no error recovery. This minimizes the processing required for each packet, allowing frame relay networks to operate at high speeds with few network delays.

Because frame relay performs only basic error checking, end stations running upper-layer protocols such as the Internet Protocol (IP) are responsible for resending packets that did not transmit correctly the first time.

Permanent Virtual Circuits

A *permanent virtual circuit* (PVC) is a dedicated logical path that connects two devices over a network. Once configured, a PVC is always available to the connected devices; a PVC does not require setup before data can travel across the network, nor does it need to be disconnected after data has passed. Since many PVCs can coexist for one physical line, devices can share the bandwidth of the transmission line.

Switched Virtual Circuits

A *switched virtual circuit* (SVC) is a logical path that is established on an as-needed basis. That is, an SVC exists only when there is data to transfer. SVCs can connect any two points on a network without the requirement that the provider preconfigure *virtual circuits* (VCs).

SVCs can provide an alternative to a large network infrastructure, potentially resulting in cost savings for networks with infrequent communications between sites. SVCs can also provide an easy and relatively inexpensive solution for disaster recovery. Costs associated with having a redundant PVC are eliminated. In addition, you can prepare an SVC network for disaster recovery by performing incremental backups to a mirror-image database on a remote server.

In addition to cost savings, SVCs provide other benefits. When frame relay networks using global addressing approach a thousand sites, they run out of data link connection identifiers (DLCIs). SVCs enable you to manage connectivity on the basis of use rather than permanent connections. Using SVCs also simplifies network administration because you do not have to preconfigure network topologies and support moves, adds, and changes, as with PVCs. This can be a significant benefit in large, highly meshed networks.

SVCs provide true bandwidth-on-demand service that can be customized based on the application in use. For example, a short interactive session might use an SVC with a low or zero committed information rate (CIR) or throughput rate, while a large file transfer of time-critical data might require an SVC at a high CIR value.

PVC and SVC Comparison

Table 1-1 lists the protocols and features that PVCs and SVCs support.

Table 1-1. PVC and SVC Protocol and Feature Support

Protocol/Feature	PVCs Support	SVCs Support
IP, IPX	✓	✓
AppleTalk APPN Bridging DECnet DLSw OSI VINES XNS	✓	
Data compression (WCP)	✓	✓
Data encryption (WEP)	✓	
Protocol prioritization	✓	✓
Dial-on-demand	✓	✓
Dial backup	✓	✓
Congestion control	✓	✓
Traffic shaping	✓	✓
PVC pass-through	✓	
Multiline	✓	

Frame Relay Packets

Figure 1-2 illustrates the structure of a frame relay packet. The packet's header field includes the following:

- *Data link connection identifier (DLCI)*

  The DLCI is the virtual circuit identification number. The frame relay network uses the DLCI to direct basic data flow. You configure the DLCI for PVCs. For SVCs, the frame relay switch assigns the DLCI number on a per call basis.

- *Command/response bit (C/R)*

  ITU-T (formerly CCITT) standards do not use this bit.

- *Forward explicit congestion notification (FECN) and backward explicit congestion notification (BECN)*

  The FECN and BECN indicate congestion on the network. For information about how the frame relay software uses these bits, see "Congestion Control," on page 1-22.

- *Discard eligibility (DE)*

  The DE bit allows the router to mark specific frames as low priority (discard eligible) before transmitting them to the frame relay network.

- *Extended address bit (EA)*

  The EA bit signals whether the next byte is part of the address. This bit indicates the last byte of the DLCI.

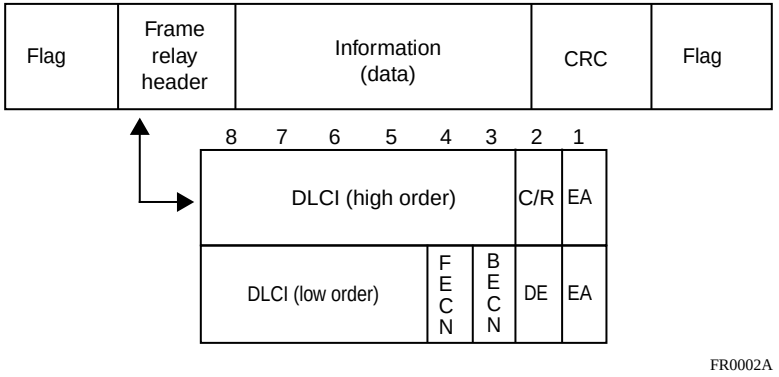

Figure 1-2. Frame Relay Header: 2-Byte Format

Figure 1-2 shows the frame relay header as a 2-byte structure. Frame relay can also format the header using 3 or 4 bytes, as shown in Figure 1-3. Note, however, that you must configure the frame relay interface on the router to use the same header length as the switched network to which it is connected.

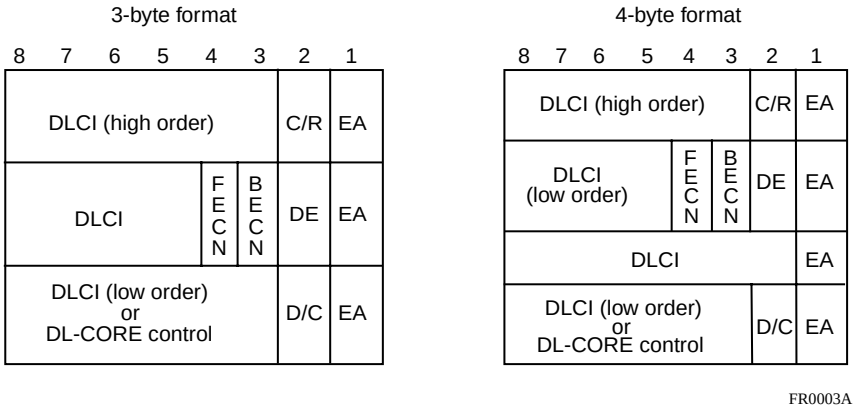

Figure 1-3. Frame Relay Header: 3- and 4-Byte Formats

Management Protocols

Frame relay is an access protocol that runs between a router or data terminal equipment (DTE) and a switch or data communications equipment (DCE). The router and the switch use the Data Link Control Management Interface (DLCMI) to exchange information about the interface and the status of each virtual circuit (Figure 1-4).

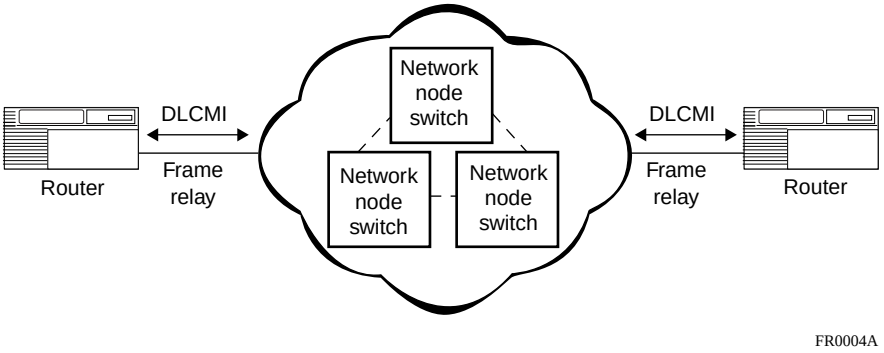

Figure 1-4. Structure of the DLCMI

DLCMI supports three standard data link management specifications: LMI, ANSI T1.617 Annex D, and CCITT (now ITU-T) Q.933 Annex A.

- The networking industry first developed the *Local Management Interface (LMI)* specification. The LMI approach is asymmetric; the router sends a status-inquiry message to the network, signaling that the router's connection to the network is functioning. The network replies with a status response.
- ANSI modified the LMI specification and incorporated it as Annex D to ANSI standard T1.617. The ANSI method is generally similar to the LMI approach.
- The CCITT (now ITU-T) modified the ANSI standard and adopted it as Annex A to Q.933. The CCITT Annex A specification is similar to Annex D, but it uses an international numbering scheme.

Be sure to configure the frame relay interface on the router to use the same management protocol as the switched network to which it is connected. For information about configuring frame relay, see Chapter 3, "Customizing Frame Relay Interfaces."

Frame Relay SVC Signaling and LAPF

Figure 1-5 shows the layers of protocol standards for frame relay signaling:

- The LAPF Core layer defines basic frame relay protocol for both PVCs and SVCs and supports the reliable transfer of multiple numbered frames over SVCs.
- The DLCMI layer defines link management protocol for PVCs.
- The LAPF and Q.933 layers define link management protocol for SVCs.

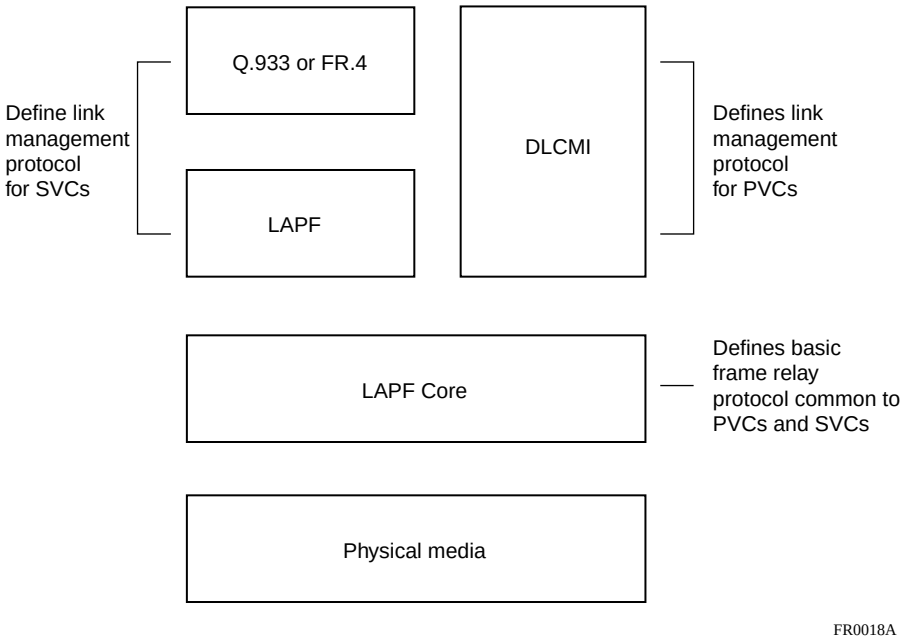

Figure 1-5. Frame Relay Signaling and LAPF Standards

The link access procedure, frame mode (LAPF) layer defines five unnumbered control frames and three numbered supervisory frames on the communications link.

LAPF defines the following categories of management frames to support reliable transfer of multiple numbered frames over SVCs:

- *Unnumbered control* -- Provides connection and disconnection services and includes set asynchronous balanced mode extended (SABME), disconnect (DISC), frame reject (FRMR), disconnected mode (DM), and unnumbered acknowledgment (UA) frames.
- *Numbered supervisory* -- Provides flow control and retransmission information and includes receiver not ready (RNR), receiver reader (RR), and reject (REJ) frames.
- *Numbered information (I)* -- A numbered command/response that passes data across the link using a sliding window protocol. The frames are numbered sequentially and carry an acknowledgment of the highest numbered frame received by the sending peer. The maximum number of frames outstanding is configurable. These frames can only be sent after setup of multiple frame communications on the link. A flag within the frame differentiates a command from its response.
- *Exchange identification (XID)* -- An unnumbered command/response used to allow peers to exchange identification information.

LAPF Operational States

LAPF has three main operational states:

- *TEI-assigned* -- The terminal endpoint identifier (TEI)-assigned state is the base interface state. When the LAPF circuit is first established, this is its state. No timers are running and only unnumbered frames are supported across the link.
- *Active* -- This state indicates that multiple frame support is up and running on the interface. Numbered information frames can travel across the link.
- *Timer recovery* -- This state indicates that a timer has expired and the peer is attempting to recover either through retransmission (T200 timeout) or by initiating an idle time handshake (T203 timeout).

Once multiple frame support is operating on the channel, numbered information frames are exchanged to transfer data and acknowledge earlier transfers.

LAPF Timeout and Retransmission Timers

Table 1-2 lists the timers and retransmission limits defined in the LAPF protocol for timeouts and retransmissions.

Table 1-2. LAPF Timeout and Retransmission Timers

Site Manager Parameter	Description
T200	This general purpose retransmission timeout is used during initiation of LAPF multiple frame support and for timeout of numbered information frames.
T203	This timeout detects excessive idle time on the line and initiates a frame handshake to check if the connection is still up.
N200	This maximum retransmission count, when reached, causes the software to take action. The action taken by the router software depends on the type of message timed out and the state of the service.

Timer T200

Timer T200 detects transmission timeouts. When a timeout occurs, the peer enters the timer recovery state and retransmits the frame, up to a maximum of N200 times. If this limit is reached, the system performs the following operations:

- Terminates multiple frame operation
- Discards all outstanding information frames
- Transitions the peer to the TEI-assigned state
- Initiates multiple frame setup

If the remote peer receives a frame that contains an error, it sends an REJ message to specify which frame was in error. In response, the local peer retransmits information frames, beginning with the bad frame.

If the remote peer encounters an error that retransmission cannot remedy, it sends an FRMR response to the local peer and transitions to the TEI-assigned state. The local peer discards all outstanding information frames, transitions to the TEI-assigned state, and initiates multiple frame setup.

The supervisory frames, RNR and RR, support flow control on the channel. If the receiver is not ready to receive data, it sends an RNR message to tell the sender to wait. When it is ready to receive data, it sends an RR message. Flow control in one direction is independent of the other direction.

Timer T203

Timer T203 is used to detect a lost connection. When either end of the link is not waiting for any data, it starts timer T203. If it sends or receives no frames before this timer expires, the peer transitions to the timer recovery state, sends either an RR or RNR message to the remote peer, and starts timer T200. If timer T200 expires, the connection is assumed lost, and the peer transitions to the TEI-assigned state.

To terminate multiple frame support on the circuit, one peer sends a DISC message to the other. The receiving peer responds with a UA message, and disconnects the circuit.

SVC Signaling

The following sections describe the signaling between a DTE and the frame relay network in which various types of messages are exchanged.

Table 1-3 contains a list of timers used in the signaling exchanges that occur. Chapter 5, “Customizing SVCs,” describes how you can use the BCC or Site Manager to configure these timers to your specific requirements.

Call Setup

A frame relay SVC is established using the frame relay signaling protocol between the subscriber (DTE) and the network. This protocol is described in the sections that follow. The timers used in this process are summarized in Table 1-3. Note that the Timer column in Table 1-3 lists the Site Manager parameter name for the timer.

Table 1-3. Network Timers

Timer	Default Timeout (secs)	State of Call	Cause for Start	Normal Stop	At First Expiration	At Second Expiration
T303	4	Call present	Outgoing setup message	Incoming connect, call proceeding, or release message	Retransmit setup message; restart timer T303	Call cleared
T305	30	Disconnect indication	Outgoing disconnect message	Incoming disconnect or release message	Network sends release message	Timer not restarted
T308	4	Release request	Outgoing release message	Incoming release or release complete message	Retransmit release message; restart timer T308	Call cleared; timer not restarted
T310	10	Incoming call proceeding	Incoming call proceeding message	Incoming connect or disconnect message	Call cleared	Timer not restarted
T322	4	Any state	Outgoing status inquiry message	Incoming status, disconnect, release, or release complete message	Retransmit status inquiry message; restart timer T322	Retransmit status inquiry message; restart timer T322

Message Processing

Table 1-4 shows how the router software handles various types of message exchanges.

Table 1-4. Message Processing

Message Type	Message Processing
Call setup	When the software receives a setup message, it performs several validations before it can deliver the message to the called subscriber and return a call proceeding message to the calling subscriber. The software must verify that all of the information fields in the message are in the proper order, all of the mandatory elements are present, and that all elements contain appropriate values.
Call proceeding	After the network determines that the setup message is valid and contains all the appropriate information, it returns a call proceeding message to the calling subscriber. When the network delivers the setup message to the called subscriber, the called subscriber may then return a call proceeding message to the network.
Connect	When the called subscriber accepts a call, it sends a connect message back to the network. The network validates the message and checks any negotiable parameters. If the message passes this inspection, the network passes the message back to the calling subscriber.
Disconnect	When a subscriber wants to terminate a call, it sends a disconnect message to the network. The network validates the messages and passes it to the peer subscriber. The cause information element is mandatory in the disconnect message. Under normal conditions, it contains a value of 16, “Normal Call Clearing.”

(continued)

Table 1-4. Message Processing *(continued)*

Message Type	Message Processing
Release	Under normal call clearing conditions, the network passes the disconnect message through the network to the remote subscriber. The subscriber receiving this disconnect message responds with a release message. The network validates the release message and passes it to the local subscriber.
Release complete	Once the network receives a release message from the subscriber and verifies it, the network returns a release complete message to the subscriber. After receiving the release message from the network, the subscriber responds with a release complete message.

Frame Relay Service Records

The router software uses service records to define frame relay circuits. A *service record* is a data structure that allows flexible grouping and characterization of VCs. A service record can contain a single PVC or SVC, multiple PVCs or SVCs, or a combination of PVCs and SVCs.

Service records:

- Simplify network addressing for VCs because you define and associate only one protocol address with groups of frame relay VCs.
- Allow multiple groups of VCs per frame relay interface.
- Enable you to group multiple VCs for each network protocol into separate service records, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.
- Conserve resources because they require a small number of circuits.
- Are easy to configure.

Default Service Record

The router creates the first service record automatically when you select frame relay as your WAN protocol. This first service record is the default service record. Any VCs not associated with another configured service record use the default service record.

Multiple Service Records

Interfaces can have multiple service records, and each service record can contain multiple PVCs, SVCs, or combinations of PVCs and SVCs.

Adding and Moving PVCs

You can add PVCs to a service record either individually, or in a range. You can also move PVCs on the same interface from one service record to another individually or as a group. For instructions, see “Deleting Frame Relay” on page 3-12.

Frame Relay Access Modes

Nortel Networks describes frame relay PVCs in terms of three access modes: group, direct, and hybrid. The following topics define each of these modes within the context of service records.

Group Access Mode

Group mode describes a service record with multiple VCs. It represents a true point-to-multipoint circuit. In group access mode, upper-layer protocols treat each frame relay network interface as a single access point to the switched network. The upper-layer protocols use a single network address to send all traffic destined for the switched network to the frame relay network interface.

When you configure each router, you assign only one network address (for example, an IP or IPX address) to the frame relay interface, not to each VC. The Data Link Control Management Interface (DLCMI) dynamically configures VCs on the default service record; you do not need to explicitly configure them.

Service records in group mode:

- Allow multiple groups of PVCs per frame relay connection.
- Enable you to gather multiple VCs for each network protocol into a separate group or service record, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.

Direct Access Mode

Direct mode describes a service record with one PVC. In direct access mode, upper-layer protocols treat the frame relay network as a series of point-to-point connections. The upper-layer protocols view each PVC as an individual network interface.

Service records in direct access mode:

- Limit broadcasts to one PVC.
- Enable multiple layer 3 networks per interface.

Hybrid Access Mode

Hybrid access mode, as its name implies, combines characteristics of group and direct access modes. Frame relay hybrid mode enables you to use the same PVCs for both routing and bridging. It works only for non-fully meshed network configurations that use:

- Both bridging and routing over a single frame relay interface
- Spanning tree bridging

In a *fully meshed* network, PVCs exist between each pair of nodes in the network. In a *non-fully meshed* network, PVCs exist only between nodes that need to communicate. Figure 1-6 shows a non-fully meshed network using hybrid mode.

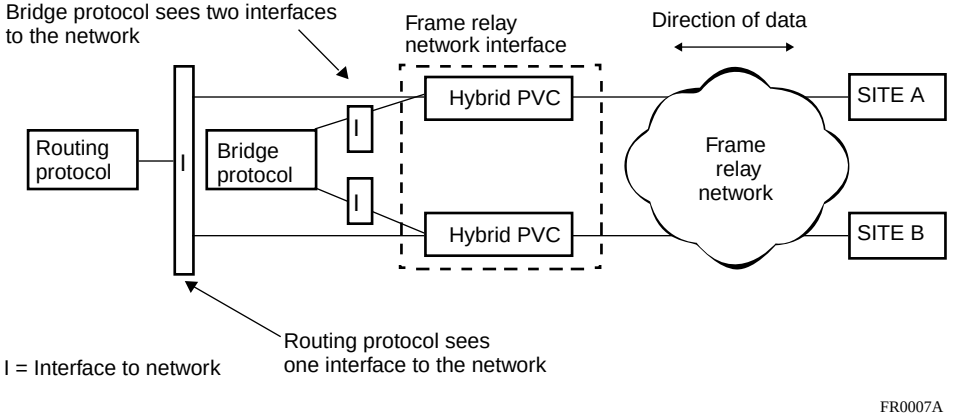

Figure 1-6. Hybrid Mode Configuration, Non-Fully Meshed Network

Using Hybrid Mode for Transparent Bridging

Figure 1-7 shows bridged traffic between site A and site B. The bridge (router 1) is running on the frame relay interface, and its configuration does not use hybrid mode.

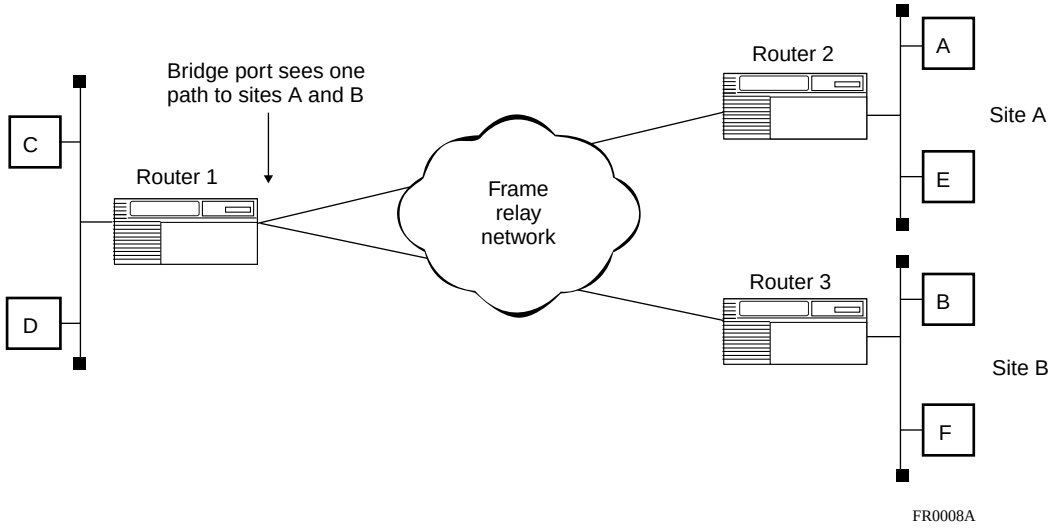

Figure 1-7. Example of a Bridged Network

In this example, the bridge receives data from site A. If the bridge does not recognize the destination address, it tries to direct traffic through another bridge port. However, without hybrid access mode configured, the frame relay bridge port views the paths to site A and site B as the same path. Because the bridge does not send out data on the same port from which it just received data, the bridge does not direct the data to site B. In this case, you should use hybrid access mode.

If you define the PVCs in hybrid mode (see Figure 1-6 on page 1-16), each PVC acts as a separate bridge port. This enables the bridge running on the frame relay interface to view the traffic from site A as arriving on a different port than that of site B. When the bridge sends out data, it sends it out from all ports, including the port that has access to site B. Therefore, data from site A can reach site B.

You configure hybrid mode by enabling the Hybrid Mode parameter for PVCs. For instructions, see “Configuring Hybrid Mode for PVCs” on page 4-12.

Source Routing

Source routing is the method by which a bridge sends data across two networks. The router supports source routing over frame relay networks, using RFC 1490 standard frame relay data encapsulation.

To configure source routing, see *Configuring Bridging Services*.

RFC 1490

RFC 1490 defines the encapsulation method for sending data across a frame relay network. Nortel Networks routers implement RFC 1490 for all protocols that Nortel Networks supports over frame relay networks.

Address Resolution for PVCs

Address resolution for PVCs maps a remote network address such as an IP address to a local DLCI number. For most protocols that you configure for a frame relay interface, the router performs address resolution automatically. However, IP, AppleTalk, and VINES use the Address Resolution Protocol (ARP). ARP dynamically generates an ARP table of addresses and DLCI numbers by sending messages back and forth to each network node to gather address information. This process increases broadcast traffic across the network.

To reduce broadcast traffic for all protocols, you can configure static routes and adjacent hosts at the protocol level. This eliminates the need for the router to perform address resolution. To reduce traffic associated specifically with VINES address resolution, you can configure Inverse ARP. Inverse ARP is the default for IP over frame relay. Refer to the appropriate protocol manual for more information about static routes, adjacent hosts, and Inverse ARP.

Table 1-5 lists how the router handles address resolution for each protocol and whether you can reduce broadcast traffic by modifying the address resolution configuration.

Table 1-5. How Protocols Handle Address Resolution

Protocol	How Router Performs Address Resolution	Configuration Requirements
Bridge (including source route)	Automatic	None
IP	ARP or Inverse ARP	Configure ARP Configure Inverse ARP
DECnet IV	Automatic	None
VINES	ARP or Inverse ARP	None for ARP Inverse ARP is the default for frame relay.
Internet Packet Exchange (IPX)	Automatic	None
Xerox Networking System (XNS)	Automatic	None
AppleTalk	AppleTalk ARP	None

Address Resolution for SVCs

For SVCs, adjacent host configuration including either an E.164 or X.121 address eliminates the need for the router to do address resolution.

Traffic Control

Frame relay is unreliable. It does not include error recovery mechanisms, relying instead on the upper-layer protocols to detect and retransmit lost frames.

Hub and spoke topologies often present a “big pipe/little pipe” situation. The central or hub site has a faster link to the frame relay service because it is a point of concentration for many remote sites. The central or hub site has a “big pipe,” with, for example, a T1/E1 connection that can transmit data at rates of 1.54 Mb/s. The remote sites usually support a much lower line speed, 56 Kb/s to 64 Kb/s, or “little pipe.” Figure 1-8 illustrates this concept.

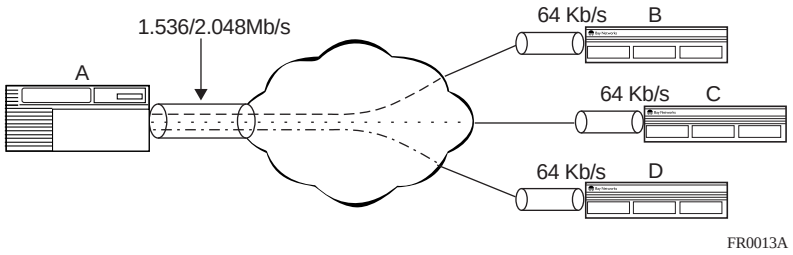

Figure 1-8. Big Pipe/Little Pipe Topology

The central site router sends traffic at its available bandwidth, in this example at T1 rates (1.536 Mb/s in the United States and Canada, 2.048Mb/s elsewhere). Some switches recognize that the remote site is configured at a lower speed, and begin to drop frames above the capacity of the remote site router. At the remote site, the frame relay interface discards frames beyond its available buffer. The assumption is that the user application detects the lost frames and either retransmits them or uses a flow control mechanism in the protocol, such as windowing, to *throttle*, which means queue, the traffic. But not all applications have a robust mechanism to deal with lost or out-of-sequence frames.

You can use Nortel Networks WAN Compression Protocol (WCP), protocol prioritization, congestion control, and traffic shaping either singly or in combination to help control the flow of traffic and avoid loss of data.

Data Compression

You can configure both hardware- and software-based data compression over WANs running frame relay.

Enabling compression improves bandwidth efficiency by eliminating redundant strings in data streams. This, in turn, improves network response times and reduces line costs. Enabling compression on a frame relay link also provides reliability. Both sides of a link using compression maintain a history of data that has already traveled across the network, and WCP detects and retransmits dropped packets.

To use data compression with frame relay, ensure that compression control is enabled (the default) and select WCP as one of the protocols for the interface. For more information about enabling compression, see “Disabling and Reenabling Data Compression for PVCs” on page 4-26. For more information about data compression, see *Configuring Data Compression Services*.

Data Encryption

Nortel Networks data encryption services enable you to protect sensitive traffic on your network. Encryption for frame relay circuits works with direct mode PVCs only. For information about and instructions for configuring data encryption, see *Configuring Data Encryption Services.*

Protocol Prioritization

You can set priorities for the traffic sent across a synchronous line interface using *protocol prioritization*, also called priority queueing. The ability to prioritize traffic is important for an application that is time-sensitive and that requires a fast response.

For example, a user at router A participating in a Telnet session with router B requires a more immediate response than does a user at router A performing a file transfer with router B.

When you select frame relay on a circuit, the router enables protocol prioritization automatically. It does so because the DLCMI packets must have a higher priority than any other packets you are sending across the network.

Enabling frame relay multiline affects protocol prioritization. For more information, see “Protocol Prioritization and Multiline Incompatibility” on page 1-37.

For information about configuring protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Congestion Control

Network congestion can degrade network performance. Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can handle. The frame relay network informs the nodes of congestion, so that they can reduce the amount of traffic across the network.

In the frame relay packet header, there are two bits that the network sets to alert nodes of network congestion. These bits, as defined by the frame relay specification, are the forward explicit congestion notation (FECN) bit and the backward explicit congestion notation (BECN) bit.

If the network detects congestion, it alerts the router in the same direction as the received frame by changing the frame's FECN bit from 0 to 1. For nodes in the opposite direction of the received frame, it changes the frame's BECN bit from 0 to 1 (Figure 1-9).

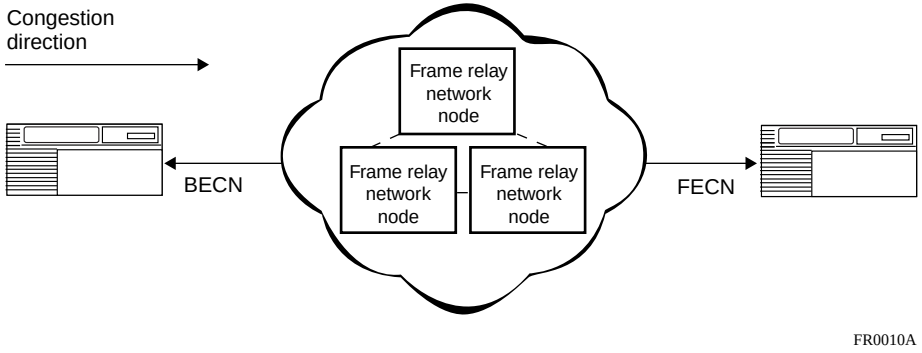

Figure 1-9. Detecting and Controlling Network Congestion

If you enable congestion control, you can specify the number of FECN/BECN bits the router receives in a given time period before it stops transmitting frames. While frames are going across the network, the frame relay interface checks received packets for FECN and BECN bits set to 1. If the interface receives the specified number of bits during the designated time period, frame relay drops all traffic destined for the PVC where there is congestion. When the interface no longer receives these congestion notifications, the router resumes transmission.

For example, suppose you set the congestion timer to 0.5 second and the congestion count to 3. In this case, if an interface receives three FECNs or BECNs within 0.5 second, the node stops sending frames (although it continues to receive frames for this PVC). If the interface receives no FECNs or BECNs during the next 0.5 second, the router resumes transmission.

If you enable congestion control and also enable traffic shaping, you can throttle, which means queue, congested traffic rather than lose it. Throttle is one of the options for the congestion method.

For instructions on configuring the congestion parameters, see “Controlling Congestion for PVCs” on page 4-15 and “Controlling Congestion for SVCs” on page 5-26.

Traffic Shaping

Traffic shaping relieves bottlenecks in topologies with high-speed connections to the central site, and low-speed connections at remote sites (Figure 1-8 on page 1-20). Committed information rate enforcement and quality of service are the major components of Nortel Networks traffic shaping.

Committed Information Rate

The *committed information rate* (CIR) is the rate at which the network supports data transfer under normal operations. Its name is descriptive: you have a contract with your carrier, who has *committed* to providing a given *throughput*, here called the committed information rate. The CIR is measured in bits per second. You configure this value that the carrier provides per virtual circuit.

When configuring the CIR, consider the following:

- CIR of 0

  You can contract with a carrier for a CIR of 0, which yields best-effort service at low cost. The carrier transmits data, but does not commit to providing a specified throughput. To configure a CIR of 0, set both the throughput (which is the CIR) and the committed burst (B_c) to 0, and set the excess burst (B_e) to a value greater than 0. For more information about burst rates, see the next section, "Committed Burst Rate and Excess Burst Rate."

- Maximum CIR

  The maximum CIR should not be greater than the speed of the access line on the slower end of a virtual circuit. In a big pipe/little pipe topology (Figure 1-8 on page 1-20), likely CIRs at the remote sites would be 32 Kb/s, 56 Kb/s, or 64 Kb/s. If you configure CIRs for these virtual circuits at the central site, you can use CIR enforcement (described in the next topic) to prevent the big pipe from sending traffic that exceeds the PVC CIRs.

- CIR enforcement

  CIR enforcement means restricting the speed of outbound traffic to a rate no faster than the CIR. It is the major component of traffic shaping. You can configure CIR enforcement to operate over Synchronous, High-Speed Serial Interface (HSSI), T1, E1, and Integrated Services Digital Network (ISDN) lines, for frame relay backup, demand, bandwidth-on-demand, and leased lines at the virtual circuit level. CIR enforcement operates on whole frames only. It controls congestion either by bringing down the virtual circuit, or by *throttling* the traffic.

Committed Burst Rate and Excess Burst Rate

The *committed burst rate* (B_c) defines the number of bits that the router can transmit over a specified time interval (T_c) when congestion is occurring. The *excess burst* (B_e) defines the number of extra bits that the router attempts to send over the T_c when there is no congestion. Both the B_c and the B_e are values that you configure.

The sum of the B_c and the B_e is the maximum amount of traffic that can travel across the network per T_c when there is no congestion. If you set the B_e to a value greater than zero, the router can send traffic exceeding the CIR. To enforce the CIR, that is, to limit traffic that the router can send to the amount of the CIR, set the B_e to 0.

If you enable congestion control *and* set the congestion method to throttle, the virtual circuit sends only B_c bits of data over the time interval T_c when congestion occurs, even if you have configured the B_e to a value greater than 0. It queues the excess data until congestion abates. If you set the congestion method to throttle-then-shutdown, the virtual circuit first queues traffic when congestion occurs, and then terminates the virtual circuit if throttling does not alleviate congestion.

To configure the committed and excess burst rates, see “Using Traffic Shaping” on page 4-21 or “Using Traffic Shaping with SVCs” on page 5-33.

Quality of Service

Quality of Service (QoS) is the second major component of Nortel Networks traffic shaping. It uses protocol prioritization with traffic shaping. You configure a prioritization filter on the default service record for the entire frame relay interface, and CIR enforcement per virtual circuit (VC). QoS operates over Synchronous, HSSI, T1, E1, and ISDN lines, for backup, demand, and for leased lines. Although the HSSI driver does not support protocol prioritization, VCs on an HSSI interface do.

Using protocol prioritization with traffic shaping creates two levels of queues. For traffic shaping the queues are high/normal/low at the VC level. For protocol prioritization they are interrupt/shaping/high/normal/low at the driver level. Figure 1-10 illustrates this concept.

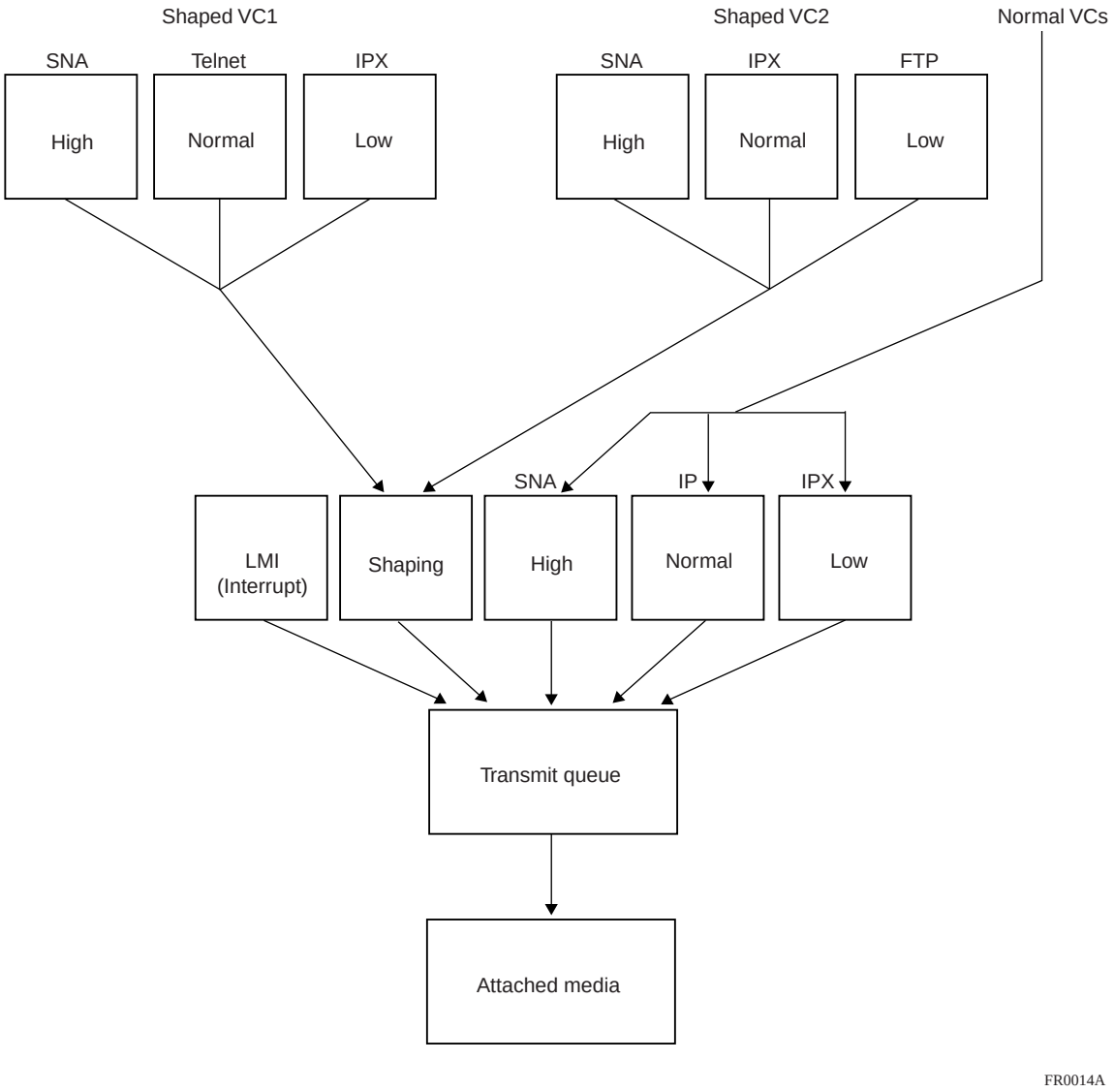

Figure 1-10. Traffic Shaping Queues

All traffic that goes to a traffic-shaped VC (VC1 or VC2) is queued as high, normal, or low priority at the VC level, and then it travels, by priority order, to a shaping queue within the driver. Normal VC traffic is queued as high, normal, or low priority at the driver level. At the driver level:

- Interrupt priority traffic, DLCMI/LMI requests (the LMI box in Figure 1-10), has the highest priority. You cannot change this.
- Shaped priority traffic (the Shaping box in Figure 1-10) has the second highest priority.
- Normal VC traffic (not shaped) has lower priority than shaped traffic. You can still prioritize normal VC traffic as high, normal, or low.

Queuing and prioritization only matter when the traffic rate exceeds the VC line rate or the CIR. If the total of all traffic is below the CIR, the router just transmits it.

You cannot prioritize between VCs on which you have enabled traffic shaping. The router schedules traffic among them in a round-robin manner.

For information about configuring filters for protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Traffic Shaping for SVCs

Traffic shaping for SVCs works according to the descriptions in the previous sections, except that SVCs derive the committed burst, excess burst, and throughput values from a combination of the traffic shaping parameters that you configure and values that the frame relay network imposes. The values that the network imposes are called *link layer core (LL Core) values*.

Requesting Quality of Service

When you configure traffic shaping for an SVC, you have several alternatives to achieve the quality of service that will best serve your network:

- You can enable SVC traffic shaping without providing values for the traffic shaping parameters. The SVCs you configure in this way use LL Core values that the network provides.

- You can enable SVC traffic shaping and provide values for the LL Core traffic shaping parameters.

  If you supply values for the LL Core parameters, the router can only request from the frame relay network an SVC with that configured quality of service. The actual values for the burst capacity and throughput that the network supplies may be less than requested because the local router, the network, and the remote end negotiate the actual quality of service. To track the values an SVC uses, use the Site Manager Statistics Manager (see *Configuring and Managing Routers with Site Manager*) or use the BCC show commands for SVCs (see Appendix C, "Monitoring Frame Relay Using the BCC show Command").

- You can disable SVC traffic shaping and provide values for the LL Core committed burst, excess burst, and throughput.

  If you configure traffic shaping this way, the router does not enforce the CIR it requests from the frame relay network. There is a risk of oversubscribing the interface, which may cause packets to be dropped.

Refining Quality of Service

You can refine quality of service requirements for SVCs. This means that you can modify traffic shaping parameters for the incoming and outgoing data flow and the minimum acceptable throughput. The values you set for these parameters depend on where the SVC call originates.

If a local router originates the call, the LL core outgoing committed burst, excess burst, and throughput values define characteristics of data the local router transmits, while the LL core incoming values define characteristics of data the local router receives.

If the local router receives a call, the outgoing values define characteristics of data the local router receives, while incoming values define characteristics of data the local router transmits.

Table 1-6 shows the direction of data and whether the incoming or outgoing parameters apply.

Table 1-6. Incoming and Outgoing

Call Originator	Direction of Data	Parameters that Apply
Local router	Outgoing to remote router	Outgoing
	Incoming from remote router	Incoming
Remote router	Incoming to local router	Outgoing
	Outgoing from local router	Incoming

For throughput, an SVC may process less throughput than it requests because the local router, the frame relay network, and the remote end of the connection negotiate quality of service. You can use the LL core minimum outgoing and minimum incoming throughput values to set the lowest throughput value the router will accept. If either the local router, the network, or the remote end cannot guarantee that value, the SVC will not be established.

To customize incoming and outgoing data flow and throughput, see “Customizing Traffic Shaping Quality of Service” on page 5-35.

Traffic Shaping Configuration Notes for PVCs and SVCs

Traffic shaping is best used at central offices to prevent the “big pipe” from sending too much data too quickly to remote sites with “little pipes.” This concept should guide your decisions about how to configure traffic shaping.

CIR Configuration Guidelines

Consider the following when you configure traffic shaping:

- In general, the value you assign to the B_c should equal 1/4 of the CIR to avoid excessive queuing and dropped packets.

  If, however, you are sending frames that exceed the size of the B_c, data travels slowly because the router must use multiple time periods to accommodate the packet size and avoid exceeding the CIR. If setting the B_c to 1/4 of the CIR yields a value lower than packet size, set the B_c to 1/3 or even 1/2 of the CIR.

  For example, a typical TFTP frame is 548 bytes. If the CIR is 16,000 bits, the B_c configured according to the 1/4 guideline would be 4,000 bits, or 500 bytes, which is not big enough to accommodate a TFTP frame.

If you set the B_c to 16,000/2, or 1/2 CIR, the result is 8,000 bits, or a packet size of 1,000 bytes, which works, but may result in excessive queuing because the T_c is 1/2 second. If you set the B_c to 16,000/3, or 1/3 CIR, the result is a B_c of 5,333 bits or 666 bytes, much closer to the 548 TFTP frame size.

- If you cannot predict the typical frame size, monitor frame relay shaping statistics for numbers of large frames and dropped frames. If either of these numbers is increasing constantly or dramatically, adjust the B_c to a higher value in small increments.

Using Data Compression and Traffic Shaping

Consider the following when you are configuring data compression and traffic shaping for your network:

- Data compression maximizes throughput and increases reliability.

  You can use compression effectively in the case of the 64 KB site that does not use traffic shaping. You can also compensate for the throughput cost associated with using compression and traffic shaping at the central site by taking into account characteristics of compression and traffic shaping, and fine-tuning traffic shaping parameters.

  -- When you configure traffic shaping, consider the compression ratio you want to achieve.

  -- If you set the B_e equal to the B_c, the router doubles the amount of traffic it attempts to send and, when you enable compression, compresses that amount of traffic, because WCP compresses data at the rate it receives it.

  -- If you also choose throttle as the congestion method, the router will queue traffic if congestion occurs, and thus prevent exceeding the CIR.

  -- Congestion may occur if compression histories are not in sync, and WCP has to resend packets. If WCP retransmits many packets, it may exceed the CIR.

- Traffic shaping increases reliability, controls congestion, and prioritizes traffic.

You can use traffic shaping at one or both ends of a link, but you must use compression at both ends of a link. It makes sense to use traffic shaping at a central site, where you have a T1 line that sends data to remote sites with 64 KB line rates, and the goal is to control the flow of traffic and avoid flooding the remote sites. However, if the CIR is equal to the line rate, which could well be the case at the remote site with 64 KB line rates, there is no need to use traffic shaping.

- Compression and traffic shaping together maximize reliability, but at the expense of throughput.

  Traffic shaping occurs at the VC level; compression, at the driver level. Shaping therefore occurs before compression, which compromises effective compression because only the precompressed traffic is shaped: the compressed traffic is not shaped. WCP compresses data at the rate it receives it, which with traffic shaping is the CIR. It is therefore unrealistic to expect a high compression throughput for data that originates from a site that also uses traffic shaping.

Oversubscribing the Traffic Shaping Interface

The CIRs that you configure are based on an average peak rate for the VCs on the network. If all VCs with traffic shaping try to send data simultaneously, they may exceed the capacity of the interface. If you oversubscribe the interface, traffic shaping will still enforce the CIR, but there may be additional latency for reserved flows. VCs without traffic shaping will send data after traffic-shaped VCs.

Queue Limits and Data Clipping

Nortel Networks routers maintain buffers for each traffic shaped VC. Each buffer can hold one frame that the router cannot send because of congestion. The router divides the number of buffers on the interface. Some facts specific to buffers are:

- The default number of buffers is 200 per interface. To change the buffer number, you can use the Technician Interface.
- The software divides the number of buffers on the interface by the number of traffic-shaped VCs, giving each VC the same number of buffers. Therefore, if you have ten traffic-shaped VCs per interface, each VC has 20 buffers.
- If you enable protocol prioritization, the default number of buffers is 30 for high priority traffic, 200 for normal, and 30 for low.

You can use the Technician Interface to increase the total number of buffers for the interface. You can also redistribute buffers among the VCs and the priority queues.

The parameters that you customize at the interface level are:

- wfFrDlcmiShapingHiQueueLimit
- wfFrDlcmiShapingNormalQueueLimit
- wfFrDlcmiShapingLoQueueLimit

The parameters you can customize at the VC level are:

- wfFrCircuitShapedHiQueueLimit.
- wfFrCircuitShapedNormalQueueLimit
- wfFrCircuitShapedLoQueueLimit

For information on using the Technician Interface, see *Using Technician Interface Software.*

Congestion Counters and Timers

The router determines congestion based on a specified number of FECN and BECN bits received during a set time period (for more information, see "Congestion Control" on page 1-22). When congestion occurs on a traffic-shaped VC, the router either drops traffic, throttles it, or throttles and then drops traffic, depending on the configured congestion method.

The FECN and BECN notifications are part of the header in a frame relay data packet. In a big pipe/little pipe topology, the central site router A typically sends much more data than it receives (Figure 1-11). This means that the remote site routers B, C, and D that receive a lot of traffic may be getting large numbers of FECNs, while the central site router is getting relatively few data packets, and therefore few BECNs, and is unaware that congestion is occurring.

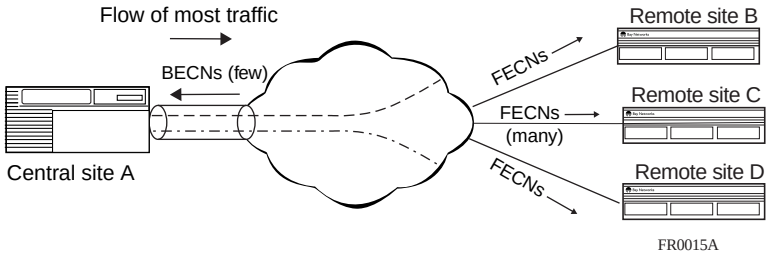

Figure 1-11. FECNs and BECNs in Big Pipe/Little Pipe Topology

You may need to modify the congestion counter and the congestion timer, from the default values of 20 FECN or BECN counts per second to, for example, 10 counts per 5 seconds to account for the differences in traffic volume to and from the central site.

X.213 Priority for SVCs

Some frame relay networks that support SVCs can prioritize SVC data and connection characters by setting X.213 priority parameters. You configure values for these parameters at the router, and the frame relay network uses them. For instructions on configuring X.213 parameters see “Setting X.213 Priorities for SVCs” on page 5-41.

Inactivity Timing for SVCs

The inactivity timer and inactivity timer mode features combine to automatically disconnect an SVC according to values that you configure for amount of time and the direction that data is flowing over the SVC. You can configure these parameters to apply to all SVCs in a service record, and you can also configure them for individual SVCs.

When the router establishes an SVC, the inactivity timer initializes two timers internal to the router: one that monitors data the router transmits, and one that monitors data the router receives. The inactivity timer mode defines how the timers restart.

Table 1-7 shows the various ways you can set these parameters, and the effect each combination has on disconnecting SVCs.

Table 1-7. Inactivity Timer and Inactivity Timer Mode Interaction

Inactivity Timer Mode	Inactivity Timers Used	Disconnect SVC
Both Directions (Site Manager) Both (BCC)	Transmit and Receive	When both timers expire (no data transmitted, *and* no data received during the timer interval).
Either Direction (Site Manager) Either (BCC)	Transmit and Receive	When either timer expires (no data transmitted *or* no data received during the timer interval).
Transmit Only (Site Manager) Outbound (BCC)	Transmit	When the transmit timer expires (no data transmitted during the timer interval).
Receive Only (Site Manager) Inbound (BCC)	Receive	When the receive timer expires (no data received during the timer interval).

For instructions on setting these values for the inactivity parameters, see “Setting Inactivity Values for SVCs” on page 5-22.

Note that a protocol priority filter configured with a no-reset action affects the operation of the inactivity timer. Normally the inactivity timer resets when the inactivity mode is set to Both or Both Directions, Either or Either Direction, or Transmit Only or Outbound. However, if the data transmitted over an SVC matches a protocol priority filter with a no-reset action, the inactivity timer will not reset. Instead, the SVC may disconnect even though data is transmitting.

Managing Routing Information Protocol (RIP) and Inactivity Timing

RIP is a mechanism that IP and IPX use to inform network devices of routing topology changes. IP and IPX let you control the frequency and destination of RIP packets. Because RIP packets can affect how the router establishes and disconnects frame relay SVCs, the software controls how RIP interacts with the frame relay SVC inactivity timer and the inactivity timer mode. For more information, see Appendix B, “RIP Management for Frame Relay SVCs.”

Multiline for PVCs

Frame relay provides a link redundancy feature called multiline, which works with frame relay PVCs. *Multiline* is a Nortel Networks proprietary implementation that lets you group two or more physical lines that back each other up in case of a failure. This ensures that information arrives at its destination on the network. In addition, if both lines are up, the router uses both lines simultaneously. Two or more physical lines must be available for a multiline configuration. Figure 1-12 illustrates a multiline configuration.

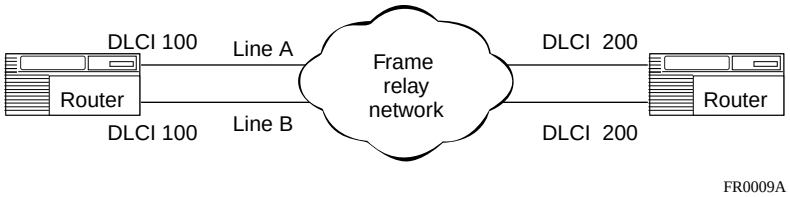

Figure 1-12. Multiline Network

In this example, when the router receives traffic destined for the network, it alternates or randomizes (depending on how you configure it) between line A and line B to transmit the data. The router uses both lines simultaneously to balance the traffic between each path. If one of these lines goes down, the router uses the remaining line.

You can create a multiline configuration of up to four service records. Each service record must be on a different physical line on the router. Each line should be on a different slot to provide fault tolerance.

You must also match DLCIs in each service record of the multiline. Matching DLCIs ensures that a backup exists for each PVC.

The most important part of configuring multiline is setting the PVC DLCI number. This number identifies each PVC, thereby specifying a path for the router to direct data to the network. For each frame relay PVC that you configure, check that PVCs with the same destination have the same DLCI number.

Note: If you use multiline, packets traveling on the two paths may arrive at their destination out of sequence. Some protocols do not tolerate packets arriving out of sequence and, as a result, you may experience poor performance or failures.

For more instruction on configuring multiline mode, see “Grouping Service Records for Multiline Mode” on page 4-27.

Traffic Distribution Between Data Paths

To distribute traffic between multiline data paths, you can use one of two methods:

- Random distribution
- Address-based distribution

Random Distribution

Random distribution means that as the router sends out each packet, it alternates between the lines. This option determines which line the packet uses based on a randomly assigned number. For each outbound packet, the router generates a random number that designates the line to use.

Random distribution balances traffic across lines and lets the router use the two lines efficiently. Because packets travel on different paths, they arrive at the destination out of sequence, and the upper-layer protocols, for example, IP and Open Systems Interconnection (OSI), have to resequence the information. Some protocols cannot tolerate packets arriving out of sequence, so be sure this option is appropriate for your application.

Address-Based Distribution

Address-based distribution determines the data path for outbound traffic from the source and destination address in each packet. Any given address pair always uses the same path.

The router determines whether to route or bridge the packet, and then uses the corresponding level of address. It uses routing-level addresses for routing traffic, and the MAC-level addresses for bridging traffic.

Address-based distribution ensures that all outbound traffic travels on the same path, and that packets arrive in sequence. For protocols that cannot receive packets out of sequence, use this method. Note, however, that this option does not always distribute traffic evenly across each line.

Protocol Prioritization and Multiline Incompatibility

You cannot use protocol prioritization with multiline. Protocol prioritization may change the order of frames arriving over a multiline interface, and frame relay multiline does not have the ability to correct the sequence.

PVC Pass-Through

The *PVC pass-through* service allows a single frame relay network access link to carry both conventional network protocol traffic and otherwise unroutable frame relay access device (FRAD) traffic. This service works with hybrid mode PVCs only. PVC pass-through connects two PVCs on separate interfaces so that the router can transmit traffic it receives on one PVC out the other with no encapsulation requirements. Figure 1-13 illustrates how PVC pass-through works.

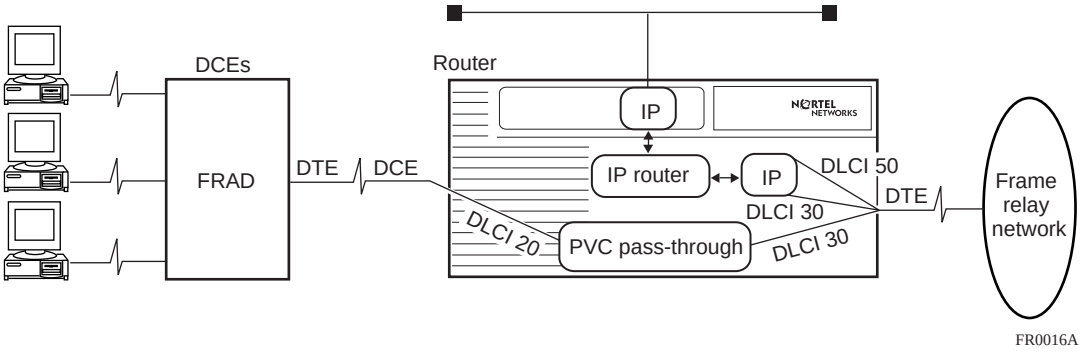

Figure 1-13. PVC Pass-Through

Figure 1-13 shows a router with an Ethernet interface and two frame relay interfaces. The interface to the frame relay network (on the right) is a DTE. The interface to the FRAD (on the left) is a DCE. The router delivers all IP frames inbound on DLCI 50 to the IP interface. It also delivers all IP frames inbound on DLCI 30 to the IP interface. The router delivers all other traffic inbound on DLCI 30 via the PVC pass-through system to DLCI 20, which transmits the data to the FRAD. All data inbound on DLCI 20 is delivered via the PVC pass-through system to DLCI 30, which transmits the data to the frame relay network.

PVC pass-through works with both leased line and dial-on-demand interfaces. It works with Nortel Networks data compression, congestion control, and traffic shaping. It does not work with data encryption, which requires a direct mode PVC.

Frame Relay Dial Services

Frame relay works with Nortel Networks dial-on-demand and dial backup services. For more information about dial services, see *Configuring Dial Services*.

Synchronous Line Configuration for Frame Relay

If you enable frame relay on a circuit, Site Manager automatically sets the following synchronous line parameters (Table 1-8):

Table 1-8. Synchronous Line Parameters for Frame Relay

Parameter	Value
BofL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	Frame Relay

For more information about these parameters, refer to *Configuring WAN Line Services*.

Calculating the MTU Size for Frame Relay Connections

The maximum transmission unit (MTU) value is the largest packet size the router will transmit across a connection. The MTU is configured as part of the WAN line parameters and its default value for frame relay is 1600.

If your Nortel Networks router communicates across a frame relay line, you may need to adjust the MTU value because as you add headers to the frame relay packet, such as those for compression and encryption, the router reduces the space for layer 3 data, such as IP or IPX datagrams.

Table 1-9 summarizes the changes you may need to make to the MTU value for your frame relay configuration. In addition to these adjustments, other router subsystems using frame relay, such as IP or IPX, may also affect the MTU value. Those adjustments are based on the particular subsystem configuration.

Table 1-9. MTU Adjustments for Frame Relay Connections

Reason for the Adjustment	Size of Overhead Packets (bytes)	Lines for which the Adjustment Applies	Notes
Data compression (WCP) overhead	3	Synchronous, MCT1, MCE1, ISDN BRI	The router always subtracts the WCP header regardless of whether WCP is enabled. Consequently, the amount of data that the router sends across the frame relay line will be less than you configured for the MTU value.
Data encryption (WEP) overhead	56	Synchronous, MCT1, MCE1, ISDN BRI	The router always subtracts the WEP header regardless of whether WCP is enabled. Consequently, the amount of data that the router sends across the frame relay line will be less than you configured for the MTU value.
Cyclic redundancy check (CRC)	2 or 4	Synchronous, MCT1, MCE1, ISDN BRI	The router always subtracts the CRC size. Consequently, the amount of data that the router sends across the frame relay line will be less than you configured for the MTU value. The default CRC value is 2.

Based on the values in Table 1-9, if you configure IP over frame relay on a synchronous line, the largest IP datagram that the router transmits is 1539. This number is determined by taking the default MTU value (1600) and subtracting the overhead packet sizes for WCP (3), WEP (56), and the CRC (2). To ensure that the router sends an IP datagram size of 1600 bytes, you must set the MTU value to 1661. For more information about the MTU parameter, see *Configuring WAN Line Services*.

Chapter 2
Starting Frame Relay

The quickest way to begin using frame relay on your network is to enable it with default values for all interface parameters and with a default service record that includes at least one permanent virtual circuit (PVC) or switched virtual circuit (SVC).

This chapter includes the following topics:

Topic	Page
Starting Configuration Tools	2-1
Preparing a Configuration File	2-2
Starting Frame Relay	2-2
Configuring PVCs and SVCs	2-4

Starting Configuration Tools

Before configuring frame relay services, see the appropriate user guide for instructions on how to use the Nortel Networks configuration tool of your choice.

Configuration Tool	User Guide
Bay Command Console (BCC™)	*Using the Bay Command Console*
Site Manager	*Configuring and Managing Routers with Site Manager*

These guides also describe generally how to create and modify a configuration.

Preparing a Configuration File

To prepare a configuration file:

1. **Create and save a configuration file that has at least one WAN interface.**
2. **Open the configuration file in local, remote, or dynamic mode.**

For information on these procedures, see *Quick-Starting Routers*.

Starting Frame Relay

You can use either the BCC or Site Manager to start frame relay using default values for all parameters. Frame relay automatically learns the necessary PVC information from the frame relay switch, and places the PVCs into the default service.

Using the BCC

To enable frame relay:

1. **Configure a physical interface on an available slot/connector.**

   To configure a physical interface on a slot and connector, navigate to the top-level box prompt and enter:

   <interface_type> **slot** *<slot_number>* **module** *<module_number>* **connector** *<connector_number>*

   interface_type is the name of a link or net module on the router.

   slot_number is the number of the slot on which the link module is located.

   module_number is the number of the module on which the slot is located.

   connector_number is the number of a connector on the link module.

   After you configure a physical interface, the BCC returns a prompt that specifies your current working location. For example, the following command configures a serial interface on slot 1, connector 2.

   ```
   box# serial slot 1 connector 2
   serial/1/2#
   ```

2. **Configure frame relay on the physical interface.**

   To configure a frame relay interface on a physical interface, navigate to the prompt for the physical interface (for example, **box; serial 1/2**) and enter:

   frame-relay

   For example:

   ```
   serial1/2# frame-relay
   frame-relay/1/2#
   ```

   You have enabled frame relay. You can now configure PVCs and SVCs as described in "Configuring PVCs and SVCs" on page 2-4. You can also specify the protocols that you want to run on this interface.

Using Site Manager

To enable frame relay, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose a link or net module with WAN interfaces, and click on one of the WAN ports, for example a COM port.	The WAN Protocols window opens.
2. Choose **Frame Relay** and click on **OK.**	The Select Protocols window opens.
3. Select the LAN protocols that you want to operate on the frame relay circuit, then click on **OK**.	Site Manager might prompt you for protocol configuration information. For instructions, see the appropriate configuration guides for those protocols that you want to run on this interface.

You have enabled frame relay. You can now configure PVCs and SVCs as described in "Configuring PVCs and SVCs" on page 2-4.

Protocol prioritization is enabled automatically when you enable frame relay. For information about protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Configuring PVCs and SVCs

You configure permanent virtual circuits (PVCs) and switched virtual circuits (SVCs) after you enable frame relay.

Configuring a PVC

You can configure PVCs using either the default service record or by adding a service record. Use these instructions to configure PVCs on the default service record. To configure PVCs on service records that you add, see "Adding PVCs to Service Records" on page 4-5.

Using the BCC

To add a PVC to the default service record, complete the following tasks:

1. **Navigate to the frame-relay prompt.**

   For example:

   ```
   box# serial/3/1; frame-relay/1/2
   ```

2. **Navigate to the default-service prompt.**

   The BCC context changes to the default service record. For example:

   ```
   frame-relay/1/2# default-service
   default-service/1/2#
   ```

3. **Enter the pvc dlci** *<value>* **command.**

   The service provider supplies the data link connection identifier (DLCI), which uniquely identifies this PVC.

   For example:

   ```
   default-service/1/2# pvc dlci 16
   pvc/1/2/16#
   ```

You have added a PVC to the default service record. Repeat this procedure to add more PVCs according to your network requirements.

Using Site Manager

To configure a PVC:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose **PVCs.**	The FR PVC List for Service window opens.
5. Choose **Add.**	The Frame Relay PVC Add window opens.
6. Set the **DLCI Number** parameter. Click on **Help** or see the parameter description on page A-25.	
7. Click on **Done.**	You return to the FR PVC List for Service window.
8. Add more PVCs as your network requires.	
9. Click on **Done** until you return to the Configuration Manager window.	

Configuring an SVC

You can configure SVCs using either the default service record or by adding a service record. Use these instructions to configure SVCs on the default service record. To configure SVCs on service records that you add, see “Adding SVC Options to Service Records” on page 5-7.

Using the BCC

To add an SVC to the default service record, complete the following tasks:

1. **Navigate to the frame-relay prompt.**

   For example:

   `box#` **serial/3/1; frame-relay/1/2**

2. **Navigate to the default-service prompt.**

   The BCC context changes to the default service record. For example:

   ```
   frame-relay/1/2# default-service
   default-service/1/2#
   ```

3. **Create an SVC by enabling SVC control.**

   For example:

   `default-service/1/2#` **svc-control enable**

4. **Specify the SVC local address.**

   For example:

   `default-service/1/2#` **svc-local-address** <*address*>

   address can be any valid X.121 or E.164 address.

   For example:

   svc-local-address e164, 1234567, 1234567, International
   svc-local-address x121, 1234567, 1234567, International

You have now added an SVC to the default service record. Repeat this procedure to add more SVCs according your network requirements.

Using Site Manager

To configure an SVC, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Set the **SVC Support** parameter to **Enable**.	The SVC parameters become available.
5. Set the following parameters: • **SVC Local Party Number** • **SVC Local Party Sub-Address** (optional) • **SVC Local Party Number Plan** • **SVC Local Party Type of Number** Click on **Help** or see the parameter descriptions beginning on page A-37.	
6. Click on **Apply**.	Site Manager replaces the Multiline button with the SVCs button in the Frame Relay Service List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Configuring Adjacent Hosts for an SVC Service Record

If you are configuring IP or IPX for a frame relay SVC, there are special considerations for configuring adjacent hosts. An adjacent host is a device on a locally attached network; it may or may not be a router. For frame relay to operate properly, the router must be able to resolve adjacent host addresses. For each adjacent host that does not implement the address resolution protocol (ARP), you need to configure a MAC address, or you must preempt the ARP process.

For more information about IP or IPX, see *Configuring IP, ARP, RARP, RIP, and OSPF Services* or *Configuring IPX Services* for instructions on configuring adjacent hosts.

Chapter 3
Customizing Frame Relay Interfaces

When you enable frame relay, default values are in effect for all parameters. Depending on your network requirements, you may want to change these values. The following sections describe how to customize frame relay for your network.

Topic	Page
Configuring Interfaces Using the BCC or Site Manager	3-1
Selecting a Management Type	3-2
Setting XOFF Control	3-4
Selecting Address Type and Length	3-5
Monitoring the Connection	3-7
Deleting Frame Relay	3-12

Configuring Interfaces Using the BCC or Site Manager

Table 3-1 lists the frame relay configuration tasks described in this chapter and indicates whether you can use the BCC or Site Manager to perform each task.

Table 3-1. Interface Configuration Tasks

Task	BCC	Site Manager
Selecting a Management Type	✓	✓
Setting XOFF Control	✓	
Selecting Address Type and Length	✓	✓
Monitoring the Connection	✓	✓
Deleting Frame Relay		✓

Selecting a Management Type

You can specify the management protocol that the router and the frame relay network use to communicate status information. Routers connected back to back also use a management protocol to exchange status information. The following list describes your options:

- *DLCMI None* provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all PVCs manually.
- *Rev 1 LMI* provides user-side management services as specified by Revision 1 of the Local Management Interface standard.
- *ANSI T1.617D* provides user-side management services as specified in Annex-D to ANSI standard T1.617-1991. This is the default value.
- *CCITT Annex A* provides user-side management services as specified by the ITU-T (formerly CCITT).
- *LMI Switch* offers limited management services for the DCE side of the connection as specified by Revision 1 of the Local Management Interface standard.
- *Annex D Switch* provides limited management services for the DCE side of the connection as specified in Annex D to ANSI standard T1.617-1991.
- *Annex A Switch* provides limited management services for the DCE side of the connection as specified by the ITU-T.

If you are connecting two routers back to back, use one of the DTE parameter options (Rev 1 LMI, ANSI T1.617D, or ITU Annex A) for the router acting as a DTE, and one of the DCE options (LMI Switch, Annex D Switch, or Annex A Switch) for the router acting as the DCE. Although you can configure the router for the DCE side of a connection, the router cannot act as a full switch, and it will not perform complete bidirectional signaling.

The LMI Switch, Annex D Switch, and Annex A Switch options are primarily for troubleshooting.

You can use either the BCC or Site Manager to select a management type.

Using the BCC

To specify a management protocol, navigate to the dlcmi prompt (for example, **box; serial/1/2; frame-relay/1/2; dlcmi**) and enter:

management-type *<value>*

value can be:

none
lmi
annex-d (the default)
annex-a
lmi-switch
annex-d-switch
annex-a-switch

For example, the following command line changes the management type from Annex D Switch to LMI Switch:

```
dlcmi/1/2# management-type lmi-switch
dlcmi/1/2#
```

Using Site Manager

To specify a management protocol, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Set the **Mgmnt Type** parameter. Click on **Help** or the see the parameter description on page A-5.	
5. Click on **Apply**.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
7. Click on **Done**.	You return to the Configuration Manager window.

Setting XOFF Control

If you choose LMI as the management protocol, you can use the BCC to configure the XOFF control. The XOFF control determines whether the router ignores or observes the XOFF bit. XOFF control is enabled by default. If you want to modify the behavior of the XOFF bit, you can disable XOFF control.

To set the XOFF control, navigate to the dlcmi prompt (for example, **box; serial/1/2; frame-relay/1/2; dlcmi**) and enter:

xoff-control *<value>*

value can be:

enabled for the router to observe the XOFF bit
disabled for the router to ignore the XOFF bit

For example, the following command line disables XOFF control:

```
dlcmi/1/2# xoff-control disabled
dlcmi/1/2#
```

Selecting Address Type and Length

You can specify the data link connection identifier (DLCI) address type and length that the router and the frame relay network use to direct packets to their destinations. The address type for the router and for the switch must be the same.

Selecting a DLCI Address Type

The options for the DLCI address type are:

- *ADDR Q922* selects addressing as specified in the final version of the Q.922 standard. Q.922 provides for FECN, BECN, DE, and EA bits. While most Q.922 addresses are included within a 2-octet field, the standard allows for 3- and 4-octet address fields. This is the default.
- The *November draft of ADDR Q922* differs from ADDR Q922 in dropping the D/C bit from the extended (3- and 4-byte) forms. The D/C bit (DLCI or DL-Core Control Indication) is always 0.
- The *March draft of ADDR Q922* differs from ADDR Q922 in defining an 11-bit DLCI and dropping the DE bit from the second octet of the address field.
- *ADDR Q921* differs from ADDR Q922 MARCH 90 in that it does not use FECNs or BECNs, which means that it does not provide congestion control.

Selecting a DLCI Address Length

The options for the DLCI address length are 2, 3, or 4 bytes. To understand the distinctions among these byte formats, see the illustrations of frame relay headers in Figure 1-2 and Figure 1-3 on page 1-6.

You can use either the BCC or Site Manager to configure the DLCI address type and length.

Using the BCC

To specify the address type, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

address-type *<value>*

value can be:

q922-march
q922-november
q921
q922march90
q922november90
q922 (the default)

For example, the following command line sets the address type to q921:

```
frame-relay/1/2# address-type q921
frame-relay/1/2#
```

To specify the address length, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

address-length *<integer>*

integer is a value of 2, 3, or 4 (bytes).

For example, the following command line sets the address length to 4 bytes:

```
frame-relay/1/2# address-length 4
frame-relay/1/2#
```

Using Site Manager

To specify the address type and length, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Set the following parameters: • **Address** • **Address Length** Click on **Help** or see the parameter descriptions beginning on page A-6.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
7. Click on **Done**.	You return to the Configuration Manager window.

Monitoring the Connection

You can monitor the status of your frame relay network connection by setting:

- Time intervals for the router to send messages that verify the integrity of the link
- The number and frequency of error messages that can occur before the connection terminates

Polling Interval

The *polling interval* specifies the amount of time between status inquiry messages that the router transmits. Status inquiry messages cause a network to respond with a link integrity verification message or full status message.

Successful completion of the request/response “handshake” verifies the status of the router/frame relay network link.

The default polling interval is 10 seconds. If this value does not match what the network requests, specify a new value in the range of 5 to 30 seconds.

Note: The polling interval does not function if you set the management type to DLCMI None.

Full Enquiry Interval

The *full enquiry interval* specifies the interval between full status inquiry messages that the router transmits. Full status inquiry messages cause the network to send a full status report message, which lists all PVCs and their status (active or inactive, and new or previously established).

The default full enquiry interval value, 6, tells the router to send a full status inquiry every 6 polling intervals. For example, with a polling interval of 10 and a full enquiry interval of 6, the router transmits a full status inquiry every 60 seconds. With a polling interval of 20 and a full enquiry interval of 30, the router transmits a full status inquiry every 10 minutes (600 seconds).

Note: The full enquiry interval does not function if you set the management type to DLCMI None.

Error Threshold and Monitored Events

Error threshold and monitored events together establish a criterion to evaluate the quality of the router’s frame relay network connection. The *error threshold* is the number of faulty status messages that cause the router to terminate the connection. *Monitored events* is the number of status message exchanges, within which those faulty status messages occur.

For example, if you accept the default of 3 for the error threshold, and the default of 4 for monitored events, three status exchange errors in a sequence of four attempted exchanges brings the connection down. Similarly, if you set the error threshold to 5 and monitored events to 10, five status exchange errors in a continuous sequence of 10 attempted exchanges brings the connection down.

Note: The error threshold and monitored events do not function if you set the management type to DLCMI None.

You can use either the BCC or Site Manager to specify error threshold and monitored events.

Using the BCC

To specify values for the polling interval, error threshold, full enquiry interval, and monitored events, see the following sections.

Polling Interval

To set the polling interval, navigate to the dlcmi prompt (for example, **box; serial/1/2; frame-relay/1/2; dlcmi**) and enter:

polling-interval <*integer*>

integer is the polling interval, from 5 to 30 seconds. The default is 10.

For example, the following command line changes the polling interval from 10 to 20 seconds:

```
dlcmi/1/2# polling-interval 20
dlcmi/1/2#
```

Full Enquiry Interval

To set the full enquiry interval, navigate to the dlcmi prompt (for example, **box; serial/1/2; frame-relay/1/2; dlcmi**) and enter:

full-enquiry-interval <*integer*>

integer is the number of polling intervals that occur before the router sends a full status inquiry. The value can be 1 to 255 intervals, and the default is 6.

For example, the following command line sets the full enquiry interval to 45 seconds:

```
dlcmi/1/2# full-enquiry-interval 45
dlcmi/1/2#
```

Error Threshold

To set an error threshold, navigate to the dlcmi prompt (for example, **box; serial/1/2; frame-relay/1/2; dlcmi**) and enter:

error-threshold *<integer>*

integer is the number of status exchange errors that can occur during the number of monitored events you specify before the router brings down the connection. The value can be 1 to 5000, and the default is 3.

For example, the following command line sets the error threshold at 12 errors:

```
dlcmi/1/2# error-threshold 12
dlcmi/1/2#
```

Monitored Events

To set monitored events, navigate to the dlcmi prompt (for example, **box; serial/1/2; frame-relay/1/2; dlcmi**) and enter:

monitored-events *<integer>*

integer is the number of monitored events that together with the error threshold establishes a criterion to evaluate the quality of the router/frame relay connection. The value can be 1 to 5000 events, and the default is 4.

For example, the following command line sets the value at 10 events:

```
dlcmi/1/2# monitored-events 10
dlcmi/1/2#
```

Using Site Manager

To configure the polling interval, error threshold, full enquiry interval, and monitored events, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Set the following parameters: • **Polling Interval** • **Full Enquiry Interval** • **Error Threshold** • **Monitored Events** Click on **Help** or see the parameter descriptions beginning on page A-7.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
7. Click on **Done**.	You return to the Configuration Manager window.

Deleting Frame Relay

To delete a frame relay service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Select a service record, then click on **Delete.**	A confirmation window opens and prompts: `Do you REALLY want to delete the FR service record?`
5. Click on **OK**.	The confirmation window closes and Site Manager removes the record from the list.
6. Click on **Done**.	You return to the Configuration Manager window.

To delete frame relay from *all* interfaces and service records, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Delete Frame Relay**.	A confirmation window opens and prompts: `Do you REALLY want to delete Frame Relay?`"
4. Click on **OK**.	The confirmation window closes. You return to the Configuration Manager window.

Chapter 4
Customizing PVCs

When you enable frame relay, default values are in effect for all Bay Command Console (BCC) and Site Manager parameters (for Site Manager parameter descriptions, see Appendix A, “Site Manager Parameters”). Depending on your network requirements, you may want to change these values. The following sections describe how to customize frame relay for your network.

Topic	Page
Configuring PVCs Using the BCC or Site Manager	4-2
Adding Service Records	4-3
Adding PVCs to Service Records	4-5
Deleting PVCs from Service Records	4-7
Moving PVCs from One Service Record to Another	4-9
Enabling Multicast	4-10
Configuring Hybrid Mode for PVCs	4-12
Configuring PVC Pass-Through	4-13
Controlling Congestion for PVCs	4-15
Using Traffic Shaping	4-21
Disabling and Reenabling Data Compression for PVCs	4-26
Grouping Service Records for Multiline Mode	4-27

Configuring PVCs Using the BCC or Site Manager

Table 4-1 lists the PVC configuration tasks described in this chapter and indicates whether you can use the BCC or Site Manager to perform each task.

Table 4-1. PVC Configuration Tasks

Task	BCC	Site Manager
Adding Service Records	✓	✓
Deleting Service Records	✓	✓
Adding PVCs to Service Records	✓	✓
Deleting PVCs from Service Records	✓	✓
Moving PVCs from One Service Record to Another		✓
Enabling Multicast	✓	✓
Configuring Hybrid Mode for PVCs		✓
Configuring PVC Pass-Through		✓
Controlling Congestion for PVCs	✓	✓
Using Traffic Shaping	✓	✓
Disabling and Reenabling Data Compression for PVCs	✓	✓
Grouping Service Records for Multiline Mode		✓

Adding Service Records

A *service record* is a data structure that allows flexible grouping and characterization of PVCs. You can add and delete service records from your frame relay interfaces. When you add a new service record, it automatically creates one PVC to which you must assign a DLCI number.

Using the BCC

To add a service record, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

service *<service_name>*

service_name identifies the service record.

For example, the following command line creates a service record with the name "boston":

```
frame-relay/1/2# service boston
service/boston#
```

Using Site Manager

To add a service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **Add**.	The Frame Relay Service Add window opens.

(continued)

5. Set the **DLCI Number** parameter. Click on **Help** or see the parameter description on page A-25. Note that Site Manager automatically configures the **Service Name** parameter.	

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **OK.**	You return to the Frame Relay Service List window.
7. Add more service records as your network requires by repeating steps 4 through 6. When you are finished, click on **Done.**	You return to the Frame Relay Circuit Definition window.
8. Click on **Done**.	You return to the Configuration Manager window.

Deleting Service Records

You can use either the BCC or Site Manager to delete service records for PVCs.

Using the BCC

To delete a service record, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

delete service/*<service_name>*

service_name identifies the service record.

For example, the following command line deletes a service record with the name "dallas":

```
frame-relay/1/2# delete service/dallas
frame-relay/1/2#
```

Using Site Manager

While frame relay is enabled, you can delete any individual service record except the default service record.

To delete a frame relay service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Select a service record, then click on **Delete.**	Site Manager displays a confirmation window that prompts: `Do you REALLY want to delete the FR service record?`
5. Click on **OK**.	The confirmation window closes and Site Manager removes the record from the list.
6. Click on **Done**.	You return to the Configuration Manager window.

Adding PVCs to Service Records

You can use either the BCC or Site Manager to add PVCs to existing service records.

Using the BCC

You can add PVCs to a service record one at a time, or add several PVCs at the same time.

To add one PVC, navigate to the prompt for the service record to which you want to add the PVCs (for example, **box; serial/1/2; frame-relay/1/2; service/boston**) and enter:

pvc *<DLCI_number>*

For example, the following command line creates a PVC with a DLCI of 20:

```
service/boston# pvc 20
pvc/3/2/20#
```

To add more than one PVC, navigate to the prompt for the service record to which you want to add PVCs (for example, **box; serial/1/2; frame-relay/1/2; service/4.0.32**) and enter:

pvc *<DLCI_number>*; **pvc** *<DLCI_number>*; **pvc** *<DLCI_number>*; ...

For example, the following command line creates PVCs with DLCI numbers 20, 21, 22, 23, and 24:

```
service/boston# pvc 20; pvc 21; pvc 22; pvc 23; pvc 24;
pvc/3/2/24#
```

Note that the working context is now that of the PVC you created last.

Using Site Manager

You can add PVCs either individually or in a range. If you want to add one PVC, enter one DLCI number. If you want to add several PVCs, enter the appropriate range of DLCI numbers in the format *<lowest_DLCI_number> - <highest_DLCI_number>*.

To add PVCs, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on **Add**.	The Frame Relay PVC Add window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Set the **DLCI Number** parameter. If you want to add more than one PVC, enter a range of numbers in the format: *<lowest_DLCI_number> - <highest_DLCI_number>.* Click on **Help** or see the parameter description on page A-25.	
7. Click on **OK**.	You return to the FR PVC List for Service window. This window now lists the PVCs you have just created.
8. Click on **Done** until you return to the Configuration Manager window.	

Deleting PVCs from Service Records

You can delete PVCs from existing service records. After you delete a PVC, it may reappear on the list of active PVCs if the switch provider does not delete it. As soon as the switch provider removes the PVC, frame relay dynamically deletes the PVC from the list.

If the switch provider deletes a PVC that you manually configured, the circuit state is set to invalid, and the PVC remains unused until you delete it from the interface.

You can use either the BCC or Site Manager to delete PVCs from service records.

Using the BCC

To delete PVCs, navigate to the prompt for the service record that has the PVC you want to delete (for example, **box; serial/1/2; frame-relay/1/2; service/dallas**) and enter:

delete pvc/*<port_number>***/***<slot_number>***/***<DLCI_number>*

For example, the following command line deletes PVCs 51 and 52:

```
service/dallas# delete pvc/1/2/51; delete pvc/1/2/52
service/dallas#
```

Using Site Manager

To delete PVCs, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Select the PVC entry that you want to delete.	
6. Click on **Delete**.	A configuration window opens and prompts: `Do you REALLY want to delete the Frame Relay PVC?`
7. Click on **OK**.	The confirmation window closes. Site Manager removes the PVC entry from the FR PVC List for Service window.
8. Click on **Done** until you return to the Configuration Manager window.	

Moving PVCs from One Service Record to Another

You can use Site Manager to move PVCs on the same line from one service record to another. You can move PVCs to existing or to new service records.

To move PVCs, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Select the PVC entry (listed by its DLCI number) you want to move, and click on **Move**.	The Frame Relay PVC Move window opens.
6. Click on **OK**.	The FR Service Record Selection window opens.
7. Click on the target service record, and click on **Select**.	The FR Service Record Selection window closes, revealing the change in the FR PVC List for Service window.
8. Click on **Done** until you return to the Configuration Manager window.	

Enabling Multicast

The multicast feature sets up a separate DLCI that replicates broadcast packets and forwards them to the appropriate destinations. You can enable support for the frame relay multicast service only if your frame relay provider offers multicasting.

You can use either the BCC or Site Manager to enable multicast service.

Using the BCC

To enable multicast service, you must set the **mutlicast-control** parameter for both the interface and the PVC.

To enable multicast for the interface, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

multicast-control enabled

The default is **disabled**.

For example, the following command line enables multicast for this frame relay interface:

```
frame-relay/1/2# multicast-control enabled
frame-relay/1/2#
```

To enable multicast for the PVC, navigate to the prompt for the PVC that you want to configure as multicast (for example, **box; serial/1/2; frame-relay/1/2; service/4.0.32; pvc/1/2/51**) and enter:

multicast-control enabled

The default is **disabled**.

For example, the following command line enables multicast for this PVC:

```
pvc/1/2/51# multicast-control enabled
pvc/1/2/51#
```

Using Site Manager

To enable multicast service, you must set the Multicast parameter for both the interface and the PVC.

To enable multicast for the interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Set the **Multicast** parameter to **Enable**. Click on **Help** or see the parameter description on page A-9.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
7. Click on **Done**.	You return to the Configuration Manager window.

Then, enable multicast for the PVC by completing the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Multicast** parameter to **Multicast**. Click on **Help** or see the parameter description on page A-27.	
6. Click on **Apply**.	
7. Click on **Done** until you return to the Configuration Manager window.	

Configuring Hybrid Mode for PVCs

Hybrid mode allows you to use the same PVCs for both routing and bridging. Using Site Manager, you configure hybrid mode by setting the Hybrid Mode parameter to ON.

To configure hybrid mode, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Set the **Hybrid Mode** parameter to **ON**. Click on **Help** or see the parameter description on page A-28.	
6. Edit other parameters if you want, and click on **Apply**.	The Select Protocols window opens.
7. Click on **Cancel**.	You return to the FR PVC List for Service window.
8. Click on **Done** until you return to the Configuration Manager window.	

Configuring PVC Pass-Through

To configure PVC pass-through service, you configure PVCs with the pass-through feature. You can then create a mapping between these PVCs, provided they reside on different lines. You can use a PVC for only one pass-through mapping.

Configuring Pass-Through PVCs

To configure PVC pass-through, first configure the PVCs by completing the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. Configure at least two PVCs, using the directions in "Adding PVCs to Service Records" on page 4-5. Configure the PVCs that you plan to map to one another on different lines.	
2. Set the **Hybrid Mode** parameter to **ON**, according to the instructions in "Configuring Hybrid Mode for PVCs" on page 4-12. Complete only steps 1 through 5.	
3. Click on **Apply**.	The Select Protocols window opens.
4. Choose **FR PVC Passthru**. If you want to also configure compression at this time, choose **WCP**. Configuring any other bridging protocols will have no effect.	
5. Click on **OK**.	You return to the FR PVC List for Service window.
6. Click on **Done** until you return to the Configuration Manager window.	

Mapping Pass-Through PVCs

Create the mapping between the PVCs by completing the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **FR PVC Passthru**.	The FR PVC Passthru menu opens.
3. Choose **Mappings**.	The FR PVC Passthru Mapping List window opens.
4. Choose **Add**.	The FR PVC Passthru Mapping Add window opens. It directs you to “Select first PVC for Passthru mapping.”
5. Choose the first PVC, then click on **Select.**	The FR PVC Passthru Mapping Add window now shows a list of PVCs that you can map to the first PVC. This list consists of all PVCs that you have not already configured for a mapping, and that reside on lines other than the one for the first PVC. Site Manager prompts you to “Select second PVC for Passthru mapping.”
6. Choose the PVC that you want to map to the previously chosen PVC, then click on **Select**.	The FR PVC Passthru Mapping List window displays the mapping you just created.
7. Repeat steps 5 and 6 to create all the necessary mappings.	
8. Click on **Done**.	You return to the Configuration Manager window.

Controlling Congestion for PVCs

Congestion occurs when a node receives more frames than it can process, or sends more frames than the transmission line can transport. You can enable congestion control on your network. When you enable congestion control, the router receives congestion notification messages from the PVC experiencing congestion, and drops all outbound traffic destined for that PVC until it no longer receives congestion notifications.

When you enable congestion control, you can set the length of time during which the router counts congestion notifications. You can also set the maximum number of congestion notifications that the router can receive during this time period. If the router receives this number of congestion notifications within the time period you specify, it stops transmitting data. The router resumes transmission when it stops receiving congestion notifications.

If you use traffic shaping with congestion control, you also need to decide which congestion control method the router should use. For more information about traffic shaping, see “Using Traffic Shaping With PVCs” on page 4-21.

If you enable congestion control, all PVCs on the interface use congestion control and the values you specify for the congestion timer and congestion counter. However, you can configure PVCs individually at the service level. In this case, you can either disable congestion for an individual PVC, or select other congestion control parameters for that PVC.

Configuring Congestion Control for an Interface

You can use either the BCC or Site Manager to control congestion for an interface.

Using the BCC

To configure congestion control for the interface you must first enable congestion control. Then, you can optionally configure the congestion timer, congestion counter, and congestion method.

Congestion Control

Congestion control is disabled by default. To enable congestion control, navigate to the frame-relay interface prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-control enabled

Enabling this parameter tells the router to drop all outbound traffic destined for a congested PVC until the congestion clears. The value of this parameter affects all PVCs that you do not individually configure.

For example, the following command line enables congestion control for this frame relay interface:

```
frame-relay/1/2# congestion-control enabled
frame-relay/1/2#
```

Congestion Timer

To change the value for the congestion timer, navigate to the frame-relay prompt for the interface (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-timer *<integer>*

integer is the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications you set in the congestion counter during this interval, the router stops transmitting data.

The value can be 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, or 5 seconds. The default is 1 second.

For example, the following command line sets a congestion timer of 2.5 seconds:

```
frame-relay/1/2# congestion-timer 2.5
frame-relay/1/2#
```

Congestion Counter

To change the value for the congestion counter, navigate to the frame-relay interface prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-counter *<integer>*

integer is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

The value can be from 1 to 500 notifications. The default is 20.

For example, the following command line sets a congestion counter of 30 notifications:

```
frame-relay/1/2# congestion-counter 30
frame-relay/1/2#
```

Congestion Method

To change the value for the congestion method, navigate to the frame-relay interface prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-method *<value>*

value can be:

throttle-then-shutdown -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

shutdown -- the default, terminates the VC when congestion occurs.

throttle -- queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled.

For example, the following command line sets a congestion method of throttle:

```
frame-relay/1/2# congestion-method throttle
frame-relay/1/2#
```

Using Site Manager

To enable congestion control for the interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Interfaces**.	The Frame Relay Interface List window opens.
4. Set the following parameters: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping) Click on **Help** or see the parameter descriptions beginning on page A-9.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
7. Click on **Done**.	You return to the Configuration Manager window.

Configuring Congestion Control for Individual PVCs

You can use either the BCC or Site Manager to control congestion for individual PVCs.

Using the BCC

The following sections describe how to configure congestion control for a PVC.

Congestion Control

To enable or disable congestion control, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; dallas; pvc/1/2/51**) and enter:

congestion-control <*value*>

value can be:

enabled -- activates congestion control. The router drops all traffic destined for a congested PVC until the congestion clears.

disabled -- deactivates congestion control.

inherit -- the default, ensures that this setting for the PVC matches the setting for the frame relay interface congestion control.

For example, the following command line enables congestion control for this PVC:

```
pvc/1/2/51# congestion-control enabled
pvc/1/2/51#
```

Congestion Timer

To change the value for the congestion timer, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; dallas; pvc/1/2/51**) and enter:

congestion-timer *<integer>*

integer is the length of time, in seconds, during which the router counts congestion notifications (see "Congestion Counter" on page 4-20). If the router receives the number of congestion notifications you set in the congestion counter during this amount of time, the router stops transmitting data.

The value can be 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, or 5 seconds. The default is 1 second.

For example, the following command line sets a congestion timer of 2.5 seconds:

```
pvc/1/2/51# congestion-timer 2.5
pvc/1/2/51#
```

Congestion Counter

To change the value for the congestion counter, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; orlando; pvc/1/2/51**) and enter:

congestion-counter *<integer>*

integer is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

The counter value can be from 1 to 500 notifications. The default is 20.

For example, the following command line sets a congestion counter of 30 notifications:

```
pvc/1/2/51## congestion-counter 30
pvc/1/2/51##
```

Congestion Method

To change the value for the congestion method, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; newyork; pvc/1/2/51**) and enter:

congestion-method *<value>*

value can be:

throttle-then-shutdown -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

shutdown -- the default, terminates the VC when congestion occurs.

throttle -- queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled.

inherit -- specifies that this VC will use the value of the interface's congestion method setting.

For example, the following command line sets a congestion method of throttle:

```
pvc/1/2/51# congestion-method throttle
pvc/1/2/51#
```

Using Site Manager

To modify congestion control for individual PVCs, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Select a PVC.	
6. Set the following parameters: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping) Click on **Help** or see the parameter descriptions beginning on page A-29.	
7. Click on **Apply**.	
8. Click on **Done** until you return to the Configuration Manager window.	

Using Traffic Shaping

Traffic shaping relieves bottlenecks in networks. You enable traffic shaping by configuring the queue limits, committed burst, excess burst, and CIR (throughput) parameters. To enhance the effectiveness of traffic shaping, you may also want to modify values for the PVC congestion control and congestion method.

For more information about the interaction between these features and traffic shaping, see “Traffic Shaping Configuration Notes for PVCs and SVCs,” on page 1-29.

You can use either the BCC or Site Manager to configure traffic shaping.

Using the BCC

To enable traffic shaping, you configure the following parameters: normal-queue-limit, high-queue-limit, low-queue-limit, committed-burst, excess-burst, and throughput.

Normal, High, and Low Queue Limits

There are three queue limits for traffic shaping: the normal queue, the high queue, and the low queue. You can configure these queue limits for a frame relay interface and a PVC.

The interface queue limit is the total number of buffers that all traffic shaped PVCs in the interface's service records may place in a specific queue.

The PVC queue limit specifies the maximum number of buffers that traffic-shaped PVCs may place in a specific queue.

To change a queue limit, navigate to the interface prompt (for example, **box; serial/1/2; frame-relay/1/2**) or the appropriate PVC prompt (for example, **box; serial/1/2; frame-relay/1/2; boston; pvc/1/2/51**) and enter one of the following commands:

normal-queue-limit *<integer>*
high-queue-limit *<integer>*
low-queue-limit *<integer>*

integer can be a value from 0 to 5000.

The default for the interface is 30. The default value for the PVC is 0, inherit, which means that the PVC uses the interface's queue limit value.

Dividing the interface's queue limit by the number of traffic-shaped PVCs gives you the number of buffers that the PVC can place into the designated queue. If you set the limit to a value other than 0, that value is the number of buffers that the PVC can place into the queue.

For example, to set an interface normal queue limit of 100, navigate to the interface prompt and enter:

```
frame-relay/1/2# normal-queue-limit 100
frame-relay/1/2
```

To set a PVC normal queue limit of 40, navigate to the prompt for the PVC you want to edit and enter:

```
pvc/1/2/51# normal-queue-limit 40
pvc/1/2/51#
```

The syntax is the same for the high- and low-queue-limit commands.

Committed Burst

The committed burst rate (B_c) defines the number of bits the router can transmit over a specified time interval when congestion occurs. Typically, you should set this parameter to 1/4 the value of the CIR. However, if this VC is sending frames larger than 1/4 of the CIR, you should increase the B_c value to accommodate that frame size. You configure this value for each PVC but not for the interface.

To change the committed burst value, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; orlando; pvc/1/2/51**) and enter:

committed-burst *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a committed burst value of 4,000 bits.

```
pvc/1/2/51# committed-burst 4000
pvc/1/2/51#
```

Excess Burst

The excess burst rate (B_e) combines with the committed burst rate to determine the maximum number of bits the router can transmit over a specified time interval when there is no congestion. The excess burst plus the committed burst must be less than or equal to the line speed. You configure this value for each PVC but not for the interface.

To change the value for the excess burst, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; orlando; pvc/1/2/51**) and enter:

excess-burst *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets an excess burst value of 2,000 bits:

```
pvc/1/2/51# excess-burst 2000
pvc/1/2/51#
```

CIR (Throughput)

The CIR (committed information rate), or throughput, defines the number of bits per second your carrier guarantees the router can transmit over a specified time interval when there is no congestion. Your carrier supplies this value. You configure this value for each PVC but not for the interface.

To enter the CIR value, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; newyork; pvc/1/2/51**) and enter:

cir *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a CIR value of 5,000 bits.

```
pvc/1/2/51# cir 5000
pvc/1/2/51#
```

Using Site Manager

Using Site Manager, you can configure only the Committed Burst, the Excess Burst, and the Throughput. To configure the normal, high, and low queue limits, you must use the BCC, as described in "Normal, High, and Low Queue Limits" on page 4-22.

To enable traffic shaping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Select the appropriate service record, and click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on a PVC that you want to configure for traffic shaping.	
6. Set the following parameters: • **Committed Burst** • **Excess Burst** • **Throughput** Click on **Help** or see the parameter descriptions beginning on page A-28.	
7. Click on **Done**.	You return to the Frame Relay Service List window.
8. Click on **Done**.	You return to the Frame Relay Circuit Definition window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling Data Compression for PVCs

Compression control is enabled by default. You can use either the BCC or Site Manager to disable or reenable compression for PVCs.

Using the BCC

The **wcp-control** command specifies whether compression is enabled or disabled for a PVC. By default, compression is enabled.

To disable compression for a PVC, navigate to the prompt for the PVC you want to modify (for example, **box; serial/1/2; frame-relay/1/2; boston; pvc/1/2/51**) and enter:

wcp-control disabled

For example, the following command line disables compression for PVC 51:

```
pvc/1/2/51# wcp-control disabled
pvc/1/2/51#
```

To reenable compression, set this parameter to **enable**.

Using Site Manager

To use data compression with frame relay, first select WCP from the Protocols menu. Compression is enabled by default for individual PVCs, so you do not have to set the WCP Enable parameter to use compression.

To disable or reenable data compression, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on a port configured for frame relay.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Frame Relay Circuit Definition window opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Set the **Compression Control** parameter. Click on **Help** or see the parameter description on page A-31.	
6. Click on **Apply**.	
7. Click on **Done** until you return to the Configuration Manager window.	

Grouping Service Records for Multiline Mode

Using Site Manager, you can configure two or more service records to run in multiline mode. For information about the Nortel Networks proprietary implementation of multiline, see “Multiline for PVCs” on page 1-35.

Service records that you group for multiline must:

- Reside on two separate physical ports
- Have the same DLCI numbers
- Not use hybrid mode
- Have all PVCs configured for the same access mode (direct or group)

To configure multiline mode, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Click on **Multiline**.	The Services Multilined With window opens.
5. Click on **Add**.	The Multiline window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Choose the frame relay interface you want to configure for multiline, and click on **Select**.	The Multiline window closes. Site Manager moves the frame relay interface from the Multiline window to the Services Multilined With window.
7. Set the **Multiline Algorithm to Choose Line** parameter. Click on **Help** or see the parameter description on page A-34.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the Configuration Manager window.

Removing Multiline Services

To remove multiline services, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Click on **Multiline**.	The Services Multilined With window opens.
5. Select the frame relay interface you want to remove, and click on **Remove**.	Site Manager removes the frame relay interface.
6. Click on **Done**.	You return to the Frame Relay Service List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Chapter 5
Customizing SVCs

When you enable frame relay, default values are in effect for all parameters. Depending on your network requirements, you may want to change these values. The following sections describe how to customize frame relay for your network.

Topic	Page
Adding Service Records for SVCs	5-2
Deleting Service Records for SVCs	5-4
Call Screening and Blocking	5-5
Adding SVC Options to Service Records	5-7
Disabling SVCs	5-9
Disconnecting Active SVCs	5-10
Modifying LAPF Parameters for SVCs	5-11
Modifying Signaling Parameters for SVCs	5-17
Setting Inactivity Values for SVCs	5-22
Individual SVC Inactivity Values	5-24
Controlling Congestion for SVCs	5-26
Using Traffic Shaping with SVCs	5-33
Disabling and Reenabling Data Compression for SVCs	5-39
Setting X.213 Priorities for SVCs	5-41

You can perform each of these tasks using either the BCC or Site Manager.

Adding Service Records for SVCs

A *service record* is a data structure that allows flexible grouping and characterization of VCs. To configure service records for SVCs, you:

- Provide a name for the service record.
- Enable SVC services.
- Provide an address for the SVC.

You can also:

- Enable call screening and blocking.
- Customize the inactivity timer and mode.

You can use either the BCC or Site Manager to configure service records for SVCs.

Using the BCC

To use the BCC to configure SVCs, you must create a service record, and then enable SVC control and specify the SVC local address.

To configure SVCs, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

service *<service_name> <line_number>***.0.***<circuit_number>*

For example, the following command line creates the service record 8.0.32:

```
frame-relay/1/2# service myservice 8.0.32
myservice/8.0.32#
```

To enable SVC control, navigate to the prompt for the service record you just added (for example, **box; serial/1/2; frame-relay/1/2; service/8.0.32**) and enter:

svc-control enabled

The default is **disabled**.

For example, the following command line enables SVCs on this service record:

```
myservice/8.0.32#  svc-control enabled
myservice/8.0.32#
```

Finally, configure the local address for the service record you just added (for example, **box; serial/1/2; frame-relay/1/2; service/8.0.32**). To do so, enter:

svc-local-address <*address*>

address can be any valid X.121 or E.164 format address.

For example, the following commands specify a local address in X.121 or E.164 format:

```
myservice/8.0.32#  svc-local-address e164, 1234567, 1234567, International
myservice/8.0.32#  svc-local-address e164, 1234567, 1234567, Unknown
myservice/8.0.32#  svc-local-address x121, 1234567, 1234567, International
myservice/8.0.32#  svc-local-address e164, 1234567, 1234567, Unknown
myservice/8.0.32#
```

Using Site Manager

To add service records to a frame relay interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Set the **SVC Support** parameter to **Enable**. Click on **Help** or see the parameter description on page A-36.	The SVC parameters become available.
5. Set the following parameters: • **SVC Local Party Number** • **SVC Local Party Sub-Address** (optional) • **SVC Local Party Number Plan** • **SVC Local Party Type of Number** Click on **Help** or see the parameter descriptions beginning on page A-37.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **Apply**.	The SVC button replaces the Multiline button in the Frame Relay Service List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Deleting Service Records for SVCs

You can use either the BCC or Site Manager to delete service records for SVCs.

Using the BCC

To delete service records, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

delete service/*<service_name>*

service_name identifies the service record.

For example, the following command line deletes service record 8.0.32:

```
frame-relay/1/2# delete service/8.0.32
frame-relay/1/2#
```

Using Site Manager

To delete service records from a frame relay interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose the service record you want to delete.	
5. Click on **Delete**.	A confirmation window opens. It asks if you really want to delete the service record.
6. Click on **OK.**	Site Manager deletes the service record.
7. Click on Done.	You return to the Configuration Manager window.

Call Screening and Blocking

You can use either the BCC or Site Manager to configure call screening and blocking for a service record.

Using the BCC

The following sections describe how to screen and block incoming calls.

SVC Call Block Direction

The **svc-call-block-direction** parameter enables you to block certain types of calls on the SVC.

To set the SVC call block direction, navigate to the prompt for the service record you want to modify (for example, **box; serial/1/2; frame-relay/1/2; service/8.0.32**) and enter:

svc-call-block-direction <*value*>

value can be:

none
inbound
outbound
all

The default is **none**.

For example, the following command line blocks outbound calls on the SVC:

```
service/8.0.32#   svc-call-block-direction outbound
service/8.0.32
```

SVC Screening

The **svc-screen-control** parameter lets you screen incoming calls on this service record.

To set SVC screen control, navigate to the prompt for the service record you want to modify (for example, **box; serial/1/2; frame-relay/1/2; service/8.0.32**) and enter:

svc-screen-control <*value*>

value can be **enabled** or **disabled**. The default is disabled.

For example, the following command line enables call screening:

```
service/8.0.32#   svc-screen-control enabled
service/8.0.32#
```

SVC Screen Usage

The **svc-screen-usage** parameter enables you to allow or disallow calls from numbers in associated SVC option records. The default is **include**, to allow calls.

To set SVC screen usage, navigate to the prompt for the service record you want to modify (for example, **box; serial/1/2; frame-relay/1/2; service/8.0.32**) and enter:

svc-screen-usage <*value*>

value can be:

include -- the default, allows calls
exclude -- disallows calls

For example, the following command line disallows calls from numbers in associated SVC option records:

```
service/8.0.32#   svc-screen-usage exclude
service/8.0.32#
```

Using Site Manager

To configure call blocking and screening, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Set the following parameters: • **SVC Call Block** • **SVC InScreening Disable** • **SVC InScreening Usage** Click on **Help** or see the parameter descriptions beginning on page A-38.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Configuration Manager window.

Adding SVC Options to Service Records

You can use either the BCC or Site Manager to add SVC options to service records.

Using the BCC

To add SVC options, navigate to the service record prompt (for example, **box; serial/1/2; frame-relay/1/2;service/8.0.32**) and enter:

svc-options *<svc_name>*

svc_name identifies the SVC and can be any alphanumeric string.

For example, the following command line adds the SVC “toronto”:

```
service/8.0.32# svc-options toronto
```

Using Site Manager

To add SVCs to existing service records, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Select the service record to which you want to add SVCs, and set the **SVC Support** parameter to **Enable**. Click on **Help** or see the parameter description on page A-36.	The SVC parameters become available.
5. Set the following parameters: • **SVC Local Party Number** • **SVC Local Party Sub-Address** (optional) • **SVC Local Party Number Plan** • **SVC Local Party Type of Number** Click on **Help** or see the parameter descriptions beginning on page A-37.	
6. Click on **Apply**.	The SVC button replaces the Multiline button in the Frame Service List window
7. Click on **SVCs**.	The FR SVC Options List for Service window opens.
8. Click on **Add**.	The Frame Relay SVC Options Add window opens.
9. Set the following parameters: • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number** Click on **Help** or the see the parameter descriptions beginning on page A-42.	
10. Click on **OK**.	You return to the FR SVC Options List for Service window.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
11. Add as many SVC options as your network requires, then click on **Done**.	You return to the Frame Relay Service List window.
12. Click on **Done**.	You return to the Configuration Manager window.

Disabling SVCs

You can use either the BCC or Site Manager to disable SVCs without deleting them.

Using the BCC

To disable SVCs, navigate to the service record prompt or the record that you want to disable (for example, **box; serial/1/2; frame-relay/1/2; service/8.0.32; svc-options/toronto**) and enter:

state disabled

The default is **enabled**.

For example, the following command line disables the SVC “toronto”:

```
svc-options/toronto# state disabled
svc-options/toronto#
```

Using Site Manager

When you disable SVCs using Site Manager, you disable SVC support for an entire service record, not an individual SVC.

To disable SVCs, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVCs you want to disable, and set the **SVC Support** parameter to **Disable**.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Configuration Manager window.

Disconnecting Active SVCs

You will see the Active Calls button in Site Manager only when there is an incoming or outgoing call.

To disconnect an active SVC, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVCs you want to disconnect.	
5. Click on **SVCs**.	The FR SVC Options List for Service window opens.
6. Click on **Active Calls**.	The Frame Relay SVC Active Calls window opens.
7. Choose the DLCI of the SVC you want to disconnect.	
8. Click on **Delete**.	The SVC Active Call Delete Query window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Click on **Yes**.	The SVC disconnects. You return to the Frame Relay SVC Active Calls window.
10. Click on **Done**.	You return to the Frame Relay SVC Options List for Service window.
11. Click on **Done**.	You return to the Frame Relay Service List window.
12. Click on **Done**.	You return to the Configuration Manager window.

Modifying LAPF Parameters for SVCs

Frame relay LAPF (link access procedure, frame mode) services support the reliable transfer of multiple numbered frames over SVCs. You can use either the BCC or Site Manager to customize LAPF.

Using the BCC

You can edit the following LAPF features in the BCC, as described in this section:

- State
- Station type
- Initiation mode
- Retransmission timer
- Idle timer
- Retransmission limit
- Information limit
- Window size

State

You can enable or disable LAPF using the **state** parameter.

To change the LAPF state, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

state <*value*>

value can be **enabled** or **disabled**. The default is **enabled**.

For example, the following command line disables LAPF:

```
lapf/3/2# state disabled
lapf/3/2#
```

Station Type

The station type determines whether the interface acts as the DCE or DTE.

To change the station type, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

station-type <*type*>

type can be:

dce
dte
network-side -- LAPF communicates as a DCE
user-side -- LAPF communicates as a DTE

The default is DTE.

The DCE and DTE options are the same as network-side and user-side, respectively.

For example, the following command line sets station type to DCE:

```
lapf/3/2# station-type dce
lapf/3/2#
```

Initiation Mode

Initiation mode determines the action LAPF will take to initiate link setup by sending or holding unnumbered parameter (SABME) frames to poll the router at the other end of the connection.

To set the initiation mode, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

initiation-mode <*mode*>

mode can be:

active (the default) -- LAPF will send SABME frames and initiate link setup.

passive -- LAPF takes no action to initiate link setup.

For example, the following command line sets a passive initiation mode:

```
lapf/3/2# initiation-mode passive
lapf/3/2#
```

Retransmission Timer

The retransmission timer is used during initiation of LAPF multiple frame support, and for timeout of LAPF numbered information frames. In the event of a timeout, the sending platform retransmits the frame, up to the maximum number of times you specify for retransmission limit.

To set the retransmission timer, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

retransmission-timer *<integer>*

integer is the length of time that the router waits to receive an acknowledgment. The value can be from 1 to 1200 tenths of a second. The default is 15.

For example, the following command line sets a timer of 30 tenths of a second (3 seconds):

```
lapf/3/2# retransmission-timer 30
lapf/3/2#
```

Idle Timer

The idle timer indicates the amount of time that the router allows with no data being transmitted. In the event of a timeout, the router initiates a frame handshake to check if the connection is still up.

To set the idle timer, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

idle-timer *<integer>*

integer is the length of time that the router allows with no data being transmitted. The value can be from 1 to 120 seconds. The default is 30.

For example, the following command line sets a timer of 18 seconds:

```
lapf/3/2# idle-timer 18
lapf/3/2#
```

Retransmission Limit

The retransmission limit is the maximum number of LAPF retransmissions that can occur after the retransmission timer expires. The connection terminates if the router reaches the retransmission limit.

To set the retransmission limit, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

retransmission-limit *<integer>*

integer is the number of times that the router retransmits after the retransmission timer expires. The value can be from 1 to 20. The default is 3.

For example, the following command line sets a retransmission limit of 8 tries:

```
lapf/3/2# retransmission-limit 8
lapf/3/2#
```

Information Limit

The information limit is the maximum number of data octets allowed in the LAPF information field. The higher the number allowed, the less overhead on the system. However, a high value could exceed the system buffer size. You should accept the default value, 260.

To set the information limit, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

information-limit *<integer>*

integer is the number of octets. The value can be from 260 (the default) to 2052.

For example, the following command line sets an information limit of 350:

```
lapf/3/2# information-limit 350
lapf/3/2#
```

Window Size

The window size indicates the maximum number of outstanding numbered information (I) frames allowed across a connection. These are frames that have traveled across the link, but which the peer has not acknowledged. Each of these frames remains in a backup queue until the peer sends an acknowledge message. A longer queue adversely affects performance. You should accept the default, 7 frames.

To set the window size, navigate to the lapf prompt (for example, **box; serial/1/2; frame-relay/1/2; lapf/3/2**) and enter:

window-size *<integer>*

integer is the number of outstanding frames allowed. The value can be from 1 to 127. The default is 7.

For example, the following command line sets a window size of 45:

```
lapf/3/2# window-size 45
lapf/3/2#
```

Using Site Manager

To modify LAPF parameters, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **Interfaces**.	The Frame Relay Interface List window opens.
4. Select a service record that has SVC support enabled.	
5. Click on **LAPF**.	The FR LAPF Parameters window opens.
6. Set the following parameters: • **Enable** • **Station Type** • **Action Initiate** • **T200, Base Timer** • **T203, Idle Timer** • **N200, Max Retries** • **N201, Max Frame Size** • **K, Max Window Size** Click on **Help** or see the parameter descriptions beginning on page A-13.	
7. Click on **OK**.	You return to the Frame Relay Interface List window.
8. Click on **Done**.	You return to the Configuration Manager window.

Modifying Signaling Parameters for SVCs

A DTE and the frame relay network exchange various type of signaling messages, including incoming and outgoing call setup, call proceeding, connect and disconnect, and release messages. You can use either the BCC or Site Manager to customize signaling parameters.

Using the BCC

You can edit the following features using the BCC:

- State
- Maximum SVCs
- Setup timer
- Disconnect timer
- Release timer
- Call proceding timer
- Status enquiry timer
- Status enquiry retry

State

You can enable or disable signaling using the BCC **state** parameter.

To change the state, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

state *<value>*

value can be **enabled** or **disabled**. The default value is **enabled**.

For example, the following command line disables signaling:

```
signalling/3/2# state disabled
signalling/3/2#
```

Maximum SVCs

Maximum SVCs indicates the maximum number of simultaneous switched virtual circuits allowed on the port. The more SVCs you allow, the larger the system memory required to support them.

To set the maximum SVCs, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

maximum-svcs *<integer>*

integer is the number of SVCs allowed. The value can be from 1 to 2147483647. The default is 100.

For example, the following command line sets a maximum of 200 SVCs:

```
signalling/3/2# maximum-svcs 200
signalling/3/2#
```

Setup Timer

The setup timer indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from that subscriber. If a timeout occurs, the router retransmits the setup message and restarts the timer. If the timer expires a second time, the router clears the call.

To set the setup timer, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

setup-timer *<integer>*

integer is the number of seconds allowed. The value can be from 2 to 90 seconds. The default is 4.

For example, the following command line sets a timer of 10 seconds:

```
signalling/3/2# setup-timer 10
signalling/3/2#
```

Disconnect Timer

The disconnect timer indicates the number of seconds allowed from the time the router sends a disconnect message and receives a release message back. If a timeout occurs, the router sends a release message and enters the release request state. The timer is not restarted.

To set the disconnect timer, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

disconnect-timer *<integer>*

integer is the number of seconds allowed. The value can be from 20 to 90 seconds. The default is 30.

For example, the following command line sets a timer of 45 seconds:

```
signalling/3/2# disconnect-timer 45
signalling/3/2#
```

Release Timer

The release timer indicates the number of seconds allowed for call clearing initiated by the other end of the connection or when the disconnect timer expires. If a timeout occurs, the router retransmits the release message and restarts the timer. If the timer expires a second time, the router clears the call.

To set the release timer, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

release-timer *<integer>*

integer is the number of seconds allowed. The value can be from 2 to 90 seconds. The default is 4.

For example, the following command line sets a timer of 45 seconds:

```
signalling/3/2# release-timer 45
signalling/3/2#
```

Call Proceeding Timer

The call proceeding timer indicates the number of seconds allowed from the time the router receives a call proceeding message to the time the router receives a connect or disconnect message. In the event of a timeout, the router clears the call.

To set the release timer, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

call-proceeding-timer *<integer>*

integer is the number of seconds allowed. The value can be from 2 to 90 seconds. The default is 10.

For example, the following command line sets a timer of 45 seconds:

```
signalling/3/2# call-proceeding-timer 45
signalling/3/2#
```

Status Enquiry Timer

The status enquiry timer indicates the number of seconds allowed from the time the router sends a status inquiry message to the time the router receives an incoming status, disconnect, release, or release complete message. If a timeout occurs, the router retransmits the status inquiry and restarts the timer. This occurs for the number of times set by the status-enquiry-retry parameter, after which the router clears the call.

To set the status enquiry timer, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

status-enquiry-timer *<integer>*

integer is the number of seconds allowed. The value can be from 2 to 90 seconds. The default is 4.

For example, the following command line sets a timer of 30 seconds:

```
signalling/3/2# status-enquiry-timer 30
signalling/3/2#
```

Status Enquiry Retry

The status enquiry retry indicates the maximum number of times the router will retransmit a status inquiry message. If the router sends the maximum number of status inquiry messages and receives no response, the router clears the call.

To set the status enquiry retry, navigate to the signalling prompt (for example, **box; serial/1/2; frame-relay/1/2; signalling/3/2**) and enter:

status-enquiry-retry *<integer>*

integer is the number of retries. The value can be from 1 to 20 retries. The default is 4.

For example, the following command line sets a value of 7 retries:

```
signalling/3/2# status-enquiry-retry 7
signalling/3/2#
```

Using Site Manager

To edit signaling parameters, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Interfaces**.	The Frame Relay Interface List window opens.
4. Select a service record that has SVC support enabled.	
5. Click on **Signaling**.	The FR Signaling Parameters window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Set the following parameters: • **Signaling Control** • **Max SVCs** • **T303, Setup Message Timer** • **T305, Disconnect Timer** • **T308, Release Timer** • **T310, Call Proceding Timer** • **T322, Status Enq Retry Timer** • **N322, Status Enq Retry Max** Click on **Help** or see the parameter descriptions beginning on page A-18.	
7. Click on **OK**.	You return to the Frame Relay Interface List window.
8. Click on **Done**.	You return to the Configuration Manager window.

Setting Inactivity Values for SVCs

You can control how and when the router disconnects SVCs according to values that you configure for amount of time and the direction that data is flowing. You can set values for a service record or for individual SVCs.

You can use either the BCC or Site Manager to set inactivity values for SVCs.

Using the BCC

You can use the BCC to set values for a service record or for individual SVCs. You set both the SVC's inactivity timer and direction.

Service Record Inactivity Values

To set inactivity values for a service record, navigate to the prompt for the service record you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32**) and enter:

svc-inactivity-timer *<integer>*

integer is the length of time, in seconds, before the SVC terminates if there is no data activity in the direction specified in the **svc-inactivity-direction** parameter.

The value can be from 0 to 2147483647 seconds. The default is 60 seconds.

For example, the following command line sets the inactivity timer to 90 seconds:

```
service/8.0.32# svc-inactivity-timer 90
service/8.0.32#
```

To configure the inactivity direction, enter:

svc-inactivity-direction *<direction>*

direction can be:

both -- only data transmitted AND received by the router prevents the expiration of the inactivity timer. If the router does not transmit and receive data, the inactivity timer expires and disconnects the SVC.

outbound -- only data transmitted by the router prevents the expiration of the inactivity timer. If the router does not transmit any data, the inactivity timer expires and disconnects the SVC.

inbound -- only data received by the router prevents the expiration of the inactivity timer. If the router does not receive any data, the inactivity timer expires and disconnects the SVC.

either -- only data transmitted OR received by the router prevents the expiration of the inactivity timer. If the router does not transmit or receive data, the inactivity timer expires and disconnects the SVC.

The default is **both**.

For example, the following command line sets the inactivity direction to outbound:

```
service/8.0.32# svc-inactivity-direction outbound
service/8.0.32#
```

Individual SVC Inactivity Values

To set the inactivity timer and direction for a particular SVC, navigate to the SVC options prompt (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

inactivity-timer *<integer>*

integer integer is the length of time, in seconds, before the SVC terminates because no data has traveled over the circuit in the direction specified by the **inactivity-direction** parameter. The value can be from 0 to 2147483647 seconds. The default is 60.

For example, the following command line sets the inactivity timer to 90 seconds:

```
svc-options/toronto# inactivity-timer 90
svc-options/toronto#
```

To configure the inactivity direction, enter:

inactivity-direction *<direction>*

direction can be:

both -- only data transmitted AND received by the router prevents the expiration of the inactivity timer. If the router does not transmit and receive data, the inactivity timer expires and disconnects the SVC.

outbound -- only data transmitted by the router prevents the expiration of the inactivity timer. If the router does not transmit any data, the inactivity timer expires and disconnects the SVC.

inbound -- only data received by the router prevents the expiration of the inactivity timer. If the router does not receive any data, the inactivity timer expires and disconnects the SVC.

either -- only data transmitted OR received by the router prevents the expiration of the inactivity timer. If the router does not transmit or receive data, the inactivity timer expires and disconnects the SVC.

The default is **both**.

For example, the following command line sets the inactivity direction to outbound:

```
svc-options/toronto# inactivity-direction outbound
```

Using Site Manager

To set inactivity values for a service record, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose a service record with SVCs.	
5. Set the following parameters: • **SVC Inactivity Timer** • **SVC Inactivity Mode** Click on **Help** or see the parameter descriptions beginning on page A-39.	
6. Click on **Apply**.	
7. Click on **Done**.	You return to the Configuration Manager window.

To set the inactivity timer value and mode for a particular SVC, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose a service record with SVCs.	
5. Click on **SVCs**.	The FR SVC Options List for Service window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Choose the SVC record whose values for the following parameters match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the following parameters: • **Inactivity Timer** • **Inactivity Timer Mode** Click on **Help** or see the parameter descriptions beginning on page A-46.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done.**	You return to the Configuration Manager window.

Controlling Congestion for SVCs

Congestion occurs when a network device receives more frames than it can process, or sends more frames than the transmission line can transport. When you enable congestion control, the router receives congestion notification messages from the SVC experiencing congestion, and drops all outbound traffic destined for that SVC until it no longer receives congestion notifications.

When you enable congestion control, you can set the length of time during which the router counts congestion notifications. You can also set the maximum number of congestion notifications that the router can receive during this time period. If the router receives this number of congestion notifications within the time period you specify, it stops transmitting data. The router resumes transmission when it stops receiving congestion notifications.

If you enable congestion control, all SVCs on the interface use congestion control and the values you specify for the congestion timer and congestion counter. However, you can configure SVCs individually at the service level. In this case, you can either disable congestion for an individual SVC, or select other congestion control parameters for that SVC.

Configuring Congestion Control for an Interface

You can use either the BCC or Site Manager to control congestion for a frame relay interface.

Using the BCC

To configure congestion control for the interface you must first enable congestion control. Then, you can optionally configure the congestion timer, congestion counter, and congestion method.

Congestion Control

Congestion control is disabled by default. To enable congestion control, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-control enabled

The value can be **enabled** or **disabled**.

Enabling this parameter tells the router to drop all outbound traffic destined for a congested SVC until the congestion clears. The value of this parameter affects all SVCs that you do not individually configure.

For example, the following command line enables congestion control for this frame relay interface:

```
frame-relay/1/2# congestion-control enabled
frame-relay/1/2#
```

Congestion Timer

To change the value for the congestion timer, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-timer *<integer>*

integer is the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications you set in the congestion counter during this amount of time, the router stops transmitting data.

The value can be 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, or 5 seconds. The default is 1.

For example, the following command line sets a congestion timer of 2.5 seconds:

```
frame-relay/1/2# congestion-timer 2.5
frame-relay/1/2#
```

Congestion Counter

To change the value for the congestion counter, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-counter *<integer>*

integer is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

The value can be from 1 to 500 notifications. The default is 20.

For example, the following command line sets a congestion counter of 30 notifications:

```
frame-relay/1/2# congestion-counter 30
frame-relay/1/2#
```

Congestion Method

To change the value for the congestion method, navigate to the frame-relay prompt (for example, **box; serial/1/2; frame-relay/1/2**) and enter:

congestion-method *<value>*

value can be:

throttle-then-shutdown -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

shutdown -- the default, terminates the VC when congestion occurs.

throttle -- queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled.

For example, the following command line sets a congestion method of throttle:

```
frame-relay/1/2# congestion-method throttle
frame-relay/1/2#
```

Using Site Manager

To configure congestion control for the interface you must first enable congestion control. Then, you can optionally configure the congestion timer, congestion counter, and congestion method.

To configure congestion control for the interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Interfaces**.	The Frame Relay Interface List window opens.
4. Set the following parameters: • **Congestion Control** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping) Click on **Help** or see the parameter descriptions beginning on page A-9.	
5. Click on **Apply**.	
6. Click on **Done**.	You return to the Configuration Manager window.

Configuring Congestion Control for Individual SVCs

You can use either the BCC or Site Manager to control congestion for individual SVCs.

Using the BCC

The following sections describe how to configure congestion control for an SVC.

Congestion Control

Congestion control is disabled by default. To enable congestion control, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

congestion-control enabled

The value can be **enabled** or **disabled**.

For example, the following command line enables congestion control for this SVC:

```
svc-options/toronto# congestion-control enabled
svc-options/toronto#
```

Congestion Timer

To change the value for the congestion timer, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

congestion-timer *<integer>*

integer is the length of time, in seconds, during which the router counts congestion notifications (see "Congestion Counter" on page 5-31). If the router receives the number of congestion notifications you set in the congestion counter during this amount of time, the router stops transmitting data.

The value can be 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, or 5 seconds. The default is 1.

For example, the following command line sets a congestion timer of 2.5 seconds:

```
svc-options/toronto# congestion-timer 2.5
svc-options/toronto#
```

Congestion Counter

To change the value for the congestion counter, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

congestion-counter *<integer>*

integer is the maximum number of congestion notifications the router can receive during the congestion timer period before it stops transmitting data.

The value can be from 1 to 500 notifications. The default is 20.

For example, the following command line sets a congestion counter of 30 notifications:

```
svc-options/toronto# congestion-counter 30
svc-options/toronto#
```

Congestion Method

To change the value for the congestion method, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

congestion-method *<value>*

value can be:

throttle-then-shutdown -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

shutdown -- the default, terminates the VC when congestion occurs.

throttle -- queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled.

inherit -- uses the value set for the interface.

For example, the following command line sets a congestion method of throttle:

```
svc-options/toronto# congestion-method throttle
svc-options/toronto#
```

Using Site Manager

To configure congestion control for individual SVCs, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Click on **SVCs**.	The FR SVC Options List for Service window opens.
5. Choose the SVC record whose values for the following parameters match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number**	
6. Set the following parameters: • **Congestion Disable** • **Congestion Timer** • **Congestion Counter** • **Congestion Method** (applies only when you enable traffic shaping) Click on **Help** or see the parameter descriptions beginning on page A-53.	
7. Click on **Apply**.	
8. Click on **Done**.	You return to the Frame Relay Service List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Using Traffic Shaping with SVCs

To use traffic shaping, first you enable it. You can then customize the traffic shaping quality of service by setting the LL Core parameters specific to committed burst, excess burst, CIR (throughput). To enhance the effectiveness of traffic shaping, you may also want to edit values for the SVC congestion control and congestion method.

For more information about traffic shaping, see "Traffic Shaping Configuration Notes for PVCs and SVCs" on page 1-29.

Enabling Traffic Shaping

You can enable traffic shaping using the BCC or Site Manager.

Using the BCC

To enable traffic shaping for SVCs, you set the **traffic-shaping-control** parameter to **enabled**, but you also have these options:

- If you do not want to use traffic shaping on this SVC, accept the default, **disabled**, and do not set the CIR, committed burst, and excess burst parameters.
- To use traffic shaping and accept the quality of service (QoS) the network provides, set this parameter to **enabled**, and do not configure the CIR, committed burst, and excess burst parameters.
- To use traffic shaping, and negotiate QoS with the network, set this parameter to **enabled**, and also set the CIR, committed burst, and excess burst parameters.
- To prevent the router from enforcing the CIR, set this parameter to **disabled**, and also set the CIR, committed burst, and excess burst parameters.

For instructions on customizing the CIR, committed burst, and excess burst parameters, see "Customizing Traffic Shaping Quality of Service" on page 5-35.

To set the **traffic-shaping-control** parameter, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

traffic-shaping-control <*value*>

value can be **enabled** or **disabled**. The default is **disabled**.

For example, the following command line enables traffic shaping on this SVC:

```
svc-option/toronto# traffic-shaping-control enabled
svc-option/toronto#
```

Using Site Manager

To enable traffic shaping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVC that you want to configure for traffic shaping.	
5. Click on **SVCs**.	The FR SVC Options List for Service window opens.
6. Choose the SVC record whose values for the following parameters match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the **Traffic Shaping Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page A-55.	
8. Click on **Apply**.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Click on **Done**.	You return to the FR SVC Options List for Service window.
10. Click on **Done**.	You return to the Frame Relay Service List window.
11. Click on **Done**.	You return to the Configuration Manager window.

Customizing Traffic Shaping Quality of Service

You can use the BCC and Site Manager to customize quality of service requirements. This means that you can modify traffic shaping parameters for the incoming and outgoing committed burst rate, excess burst rate, and minimum acceptable throughput.

For more information about quality of service, see “Requesting Quality of Service” on page 1-27.

Using the BCC

To customize traffic shaping quality of service, you set values for committed burst, excess-burst, and CIR (throughput).

Committed Burst

The committed burst rate (B_c) defines the number of bits the router can transmit over a specified time interval when congestion occurs. For SVCs, you configure two parameters to define committed burst: *committed-burst-in* and *committed-burst-out*. Respectively, these are the maximum number of bits that a VC can receive and transmit during the VC’s burst period when congestion is occurring. To enable traffic shaping, these parameters and the CIR must be greater than zero. The values for the committed burst should be lower than the CIR.

To change the value for **committed-burst-in** or **committed-burst-out**, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

committed-burst-in *<integer>*

or

committed-burst-out *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a **committed-burst-in** value of 4,000 bits:

```
svc-option/toronto# committed-burst-in 4000
svc-option/toronto#
```

Excess Burst

For SVCs, you configure two parameters to define excess burst: *excess-burst-in* and *excess-burst-out*. The values for excess-burst-in combined with committed-burst-in, and for excess-burst-out combined with committed-burst-out define, respectively, the maximum number of bits that a VC can receive and transmit during the VC's burst period when no congestion is occurring. The excess burst plus the committed burst must be less than or equal to the line speed.

To change the value for **excess-burst-in** or **excess-burst-out**, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

excess-burst-in *<integer>*

or

excess-burst-out *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets an **excess-burst-in** value of 3,000:

```
svc-option/toronto# excess-burst-in 3000
svc-option/toronto#
```

CIR (Throughput)

The CIR (committed information rate), or throughput, defines the number of bits per second your carrier guarantees the router can transmit over a specified time interval when there is no congestion. For SVCs, you configure four parameters that define throughput: cir-in, cir-in-minimum, cir-out, and cir-out-minimum.

The *cir-in* and *cir-out* parameters specify the requested incoming and outgoing throughput (kbits/second) when no congestion is occurring.

The *cir-in-minimum* and *cir-out-minimum* parameters specify the minimum acceptable incoming and outgoing throughput (kbits/second).

To change the value of **cir-in** or **cir-out**, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

cir-in *<integer>*

or

cir-out *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a **cir-in** value of 10,000 bits:

```
svc-option/toronto# cir-in 10000
svc-option/toronto#
```

To change the value of **cir-in-minimum** or **cir-out-minimum**, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

cir-in-minimum *<integer>*

or

cir-out-minimum *<integer>*

integer is the number of bits the router can transmit per time interval. The value can be from 0 to 2,147,483,647 bits. The default is 0.

For example, the following command line sets a cir-in-minimum value of 10,000 bits:

```
svc-option/toronto# cir-in-minimum 10000
svc-option/toronto#
```

Using Site Manager

To customize traffic shaping quality of service, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVC you want to modify.	
5. Click on **SVCs**.	The FR SVC Options List for Service window opens.
6. Choose the SVC record whose values for the following parameters match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number**	
7. Set the following parameters: • **LL Core Out Throughput** • **LL Core In Throughput** • **LL Core Min Out Throughput** • **LL Core Min In Throughput** • **LL Core Out Committed Burst** • **LL Core In Committed Burst** • **LL Core Out Excess Burst** • **LL Core In Excess Burst** Click on **Help** or see the parameter descriptions beginning on page A-50.	
8. Click on **Apply**.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Click on **Done**.	You return to the FR SVC Options List for Service window.
10. Click on **Done**.	You return to the Frame Relay Service List window.
11. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling Data Compression for SVCs

You can use the BCC or Site Manager to disable and reenable data compression for SVCs.

Using the BCC

The **wcp-control** parameter specifies whether compression is enabled or disabled for an SVC. By default, compression is enabled.

To disable compression for an SVC, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter:

wcp-control disabled

For example, the following command line disables compression for this SVC:

```
svc-options/toronto# wcp-control disabled
svc-options/toronto#
```

To reenable compression, set this parameter back to **enable**.

Using Site Manager

To enable data compression for SVCs, first select WCP from the Protocols menu. Compression is enabled by default for individual SVCs, so you do not have to set the WCP Enable parameter to use compression. For more information about WCP, see *Configuring Data Compression Services*.

To disable or reenable compression, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that you want to configure for compression.	
5. Click on **SVCs**.	The FR SVC Options List for Service window opens.
6. Choose the SVC record whose values for the following parameters match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number** Click on **Help** or see the parameter descriptions beginning on page A-42.	
7. Set the **WCP Enable** parameter to **Disable**. Click on **Help** or see the parameter description on page A-56.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the Configuration Manager window.

Setting X.213 Priorities for SVCs

Some frame relay networks can prioritize SVC data and connection characteristics by setting X.213 priority parameters. Though you configure these parameters for the router, it is the network that uses them.

You can use either the BCC or Site Manager to set X.213 priorities for SVCs.

Using the BCC

The X.213 priority parameters adhere to ITU-T Q.933 and X.213. The parameters are **data-priority**, **data priority-minimum**, **gain-priority**, **gain-priority-minimum**, **keep-priority**, and **keep-priority-minimum**. If your network does not support X.213 prioritization, accept the default values for these parameters, unless the network is able to accept pieces of signaling information that it does not recognize.

The **data-priority** parameter sets the priority of data on the network connection. It is a value the router requests; it is not guaranteed.

The **data-priority-minimum** parameter sets the lowest acceptable priority of data on a connection.

The **gain-priority** parameter sets the priority of data required to add a connection. It is a value the router requests; it is not guaranteed.

The **gain-priority-minimum** parameter sets the lowest acceptable priority of data to add a connection. This is a value below which the router will not create the SVC.

The **keep-priority** parameter sets the priority of data required to maintain a connection. This is a value the router requests; it is not guaranteed.

The **keep-priority-minimum** parameter sets the lowest acceptable priority of data required to maintain a connection. This is a value below which the router will disconnect the SVC.

To set X.213 priority values, navigate to the prompt for the SVC you want to modify (for example, **box; serial/3/2; frame-relay/3/2; service/8.0.32; svc-options/toronto**) and enter any of the following parameters:

data-priority *<integer>*
data-priority-minimum *<integer>*
gain-priority *<integer>*
gain-priority-minimum *<integer>*
keep-priority *<integer>*
keep-priority-minimum *<integer>*

integer can be a value from 0 to 15, with 0 as the lowest priority and 14 as the highest. A value of 15 means unspecified.

For example, the following command line sets a data priority of 9 for SVC options:

```
svc-options/toronto# data-priority 9
svc-options/toronto#
```

Using Site Manager

To set X.213 priority values, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Services**.	The Frame Relay Service List window opens.
4. Choose the service record that includes the SVC that you want to configure for traffic shaping.	
5. Click on **SVCs**.	The Frame Relay SVC Options List for Service window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Choose the SVC record whose values for the following parameters match the remote end of the SVC connection. • **Remote Party Number** • **Remote Party Sub-Address** • **Remote Party Number Plan** • **Remote Party Type of Number** Click on **Help** or see the parameter descriptions beginning on page A-42.	
7. Set the following parameters: • **X.213 Data Priority** • **X.213 Data LQA Priority** • **X.213 Gain Priority** • **X.213 Gain LQA Priority** • **X.213 Keep Priority** • **X.213 Keep LQA Priority** Click on **Help** or see the parameter descriptions beginning on page A-47.	
8. Click on **Apply**.	
9. Click on **Done**.	You return to the Frame Relay Service List window.
10. Click on **Done**.	You return to the Configuration Manager window.

Appendix A
Site Manager Parameters

This appendix contains the following information:

Topic	Page
Interface Parameters	A-2
SVC LAPF Parameters	A-12
SVC Signaling Parameters	A-17
Service Name Parameter	A-22
PVC Parameters	A-24
C Service Record Parameters	A-35

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify attributes by issuing **set** and **commit** commands with the MIB Object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify attribute values you enter. Entering an invalid value can corrupt your configuration.

Interface Parameters

The Frame Relay Interface List window contains the parameters for the frame relay interfaces. If you have configured PVCs only, you see a window similar to the one in Figure A-1.

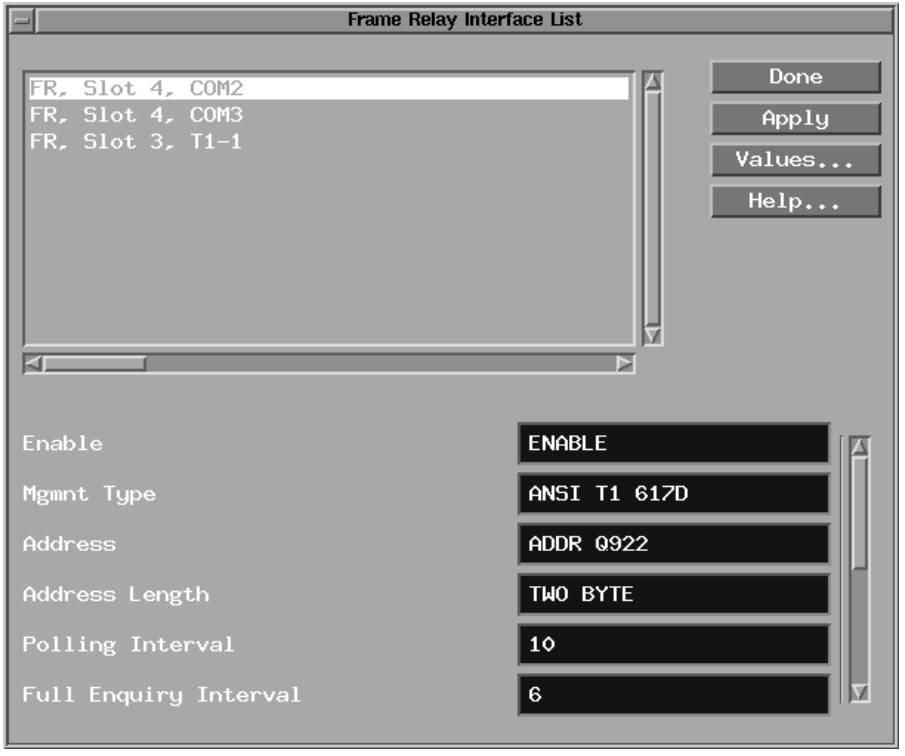

Figure A-1. Frame Relay Interface List Window (for PVCs)

If you have configured any SVCs, you see a window similar to the one in Figure A-2, which includes buttons for LAPF and Signaling.

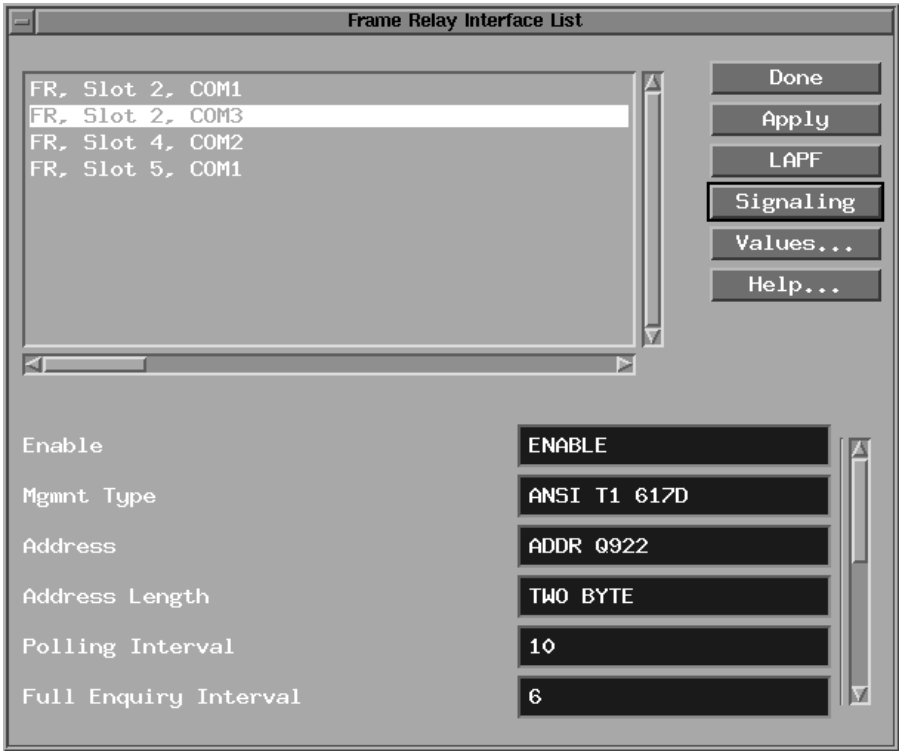

Figure A-2. Frame Relay Interface List Window (for SVCs)

To access the Frame Relay Interface List window:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Interfaces**.	The Frame Relay Interface List window opens.

Frame Relay Interface parameters are the same for PVCs and SVCs. Use the descriptions that follow when you modify these parameters.

Parameter: Enable

Path:	Configuration Manager > Protocols > Frame Relay > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables frame relay service on this interface.
Instructions:	To disable frame relay service on this interface without deleting it, set to Disable. To reenable frame relay service, if you previously disabled it, set to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.1.1.2

Parameter: Mgmnt Type

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: ANSI T1.617D

Options: DLCMI None │ Rev 1 LMI │ ANSI T1.617D │ CCITT Annex A │ LMI Switch │ Annex D Switch │ Annex A Switch

Function: Specifies the management protocol that the router and the frame relay network use to communicate status information. Routers connected back to back also use a management protocol to exchange status information.

Option for No Management

DLCMI None -- provides no management interface between the router and the frame relay network. In the absence of management support, you must configure all VCs manually.

Options for User Management

Rev 1 LMI -- provides user-side management services as specified by Revision 1 of the Local Management Interface standard.

ANSI T1.617D -- provides user-side management services as specified in Annex D to ANSI standard T1.617-1991.

CCITT Annex A -- provides user-side management services as specified by the ITU-T (formerly CCITT).

Options for Limited Management for DCE Switch (primarily for troubleshooting)

LMI Switch -- offers limited management services for the DCE side of the connection as specified by Revision 1 of the Local Management Interface standard.

Annex D Switch -- provides limited management services for the DCE side of the connection as specified in Annex D to ANSI standard T1.617-1991.

Annex A Switch -- provides limited management services for the DCE side of the connection as specified by the ITU-T.

Instructions: Select the management protocol for the frame relay network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.6

Parameter: Address

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: ADDR Q922

Options: ADDR Q922 | ADDR Q922 November 90 | ADDR Q922 MARCH 90 | ADDR Q921

Function: Specifies the DLCI addressing type.

ADDR Q922 -- selects addressing as specified in the final version of the Q.922 standard. Q.922 provides for FECN, BECN, DE, and EA bits. While most Q.922 addresses are included within a 2-octet field, the standard allows for 3- and 4-octet address fields.

The November draft of ADDR Q922 -- differs from ADDR Q922 in dropping the D/C bit from the extended (3- and 4-byte) forms.

The March draft of ADDR Q922 -- differs from ADDR Q922 in defining an 11-bit DLCI and dropping the DE bit from the second octet of the address field.

ADDR Q921 -- differs from ADDR Q922 MARCH 90 in that it does not use FECNs or BECNs.

Instructions: Select the addressing type for the frame relay interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.8

Parameter: Address Length

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Two Byte

Options: Two Byte | Three Byte | Four Byte

Function: Specifies the length of the frame relay address field.

The length of this field determines the range of valid numbers for the DLCI number. For more details, see the DLCI Number parameter description on page A-25.

Instructions: Select the address length for the address field. This must match what the network specifies.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.9

Parameter: Polling Interval

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 10

Options: 5 to 30 seconds

Function: Specifies the interval between status inquiry messages that the router transmits. Status inquiry messages cause a network response in the form of a link integrity verification message or full status message. Successful completion of the request/response "handshake" verifies the status of the router/frame relay network link.

Instructions: Accept the default value, 10 seconds. If this value does not match what the network requests, enter a value that is appropriate for your network in the range of 5 to 30 seconds. Polling Interval does not function if you set Mgmnt Type to DLCMI None.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.10

Parameter: Full Enquiry Interval

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 6

Options: 1 to 255 polling intervals

Function: Specifies the interval between full status inquiry messages that the router transmits. Full status inquiry messages cause the network to send a full status report message, which lists all VCs, the VC status (active or inactive, and new or previously established). This parameter works with the Polling Interval parameter.

The default value, 6, tells the router to send a full status inquiry every 6 polling intervals. For example, with a polling interval of 10 and a full enquiry interval of 6, the router transmits a full status inquiry every 60 seconds; with a polling interval of 20 and a full enquiry interval of 30, the router transmits a full status inquiry every 10 minutes (600 seconds).

Instructions: Enter a value from 1 to 255, according to what the network dictates. Full Enquiry Interval does not function if you set Mgmnt Type to DLCMI None.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.11

Parameter: Error Threshold

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 3

Options: 0 to 2147483647

Function: Together with the value of the Monitored Events parameter, establishes a criterion to evaluate the quality of the router/frame relay network connection.

If you accept the default values for both Error Threshold and Monitored Events, three status exchange errors in a sequence of four attempted exchanges will bring the connection down. With Error Threshold set to 5 and Monitored Events set to 10, five status exchange errors in a continuous sequence of 10 attempted exchanges will bring the connection down.

After the network clears the connection, status exchanges continue, and the router monitors line integrity. When the number of consecutive, successful status exchanges is equal to the Error Threshold value, the router restores the frame relay connection.

Error Threshold and Monitored Events are nonfunctional if you set Mgmnt Type to DLCMI None.

Instructions: Enter the number of faulty status exchanges that will bring the connection down.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.12

Parameter: Monitored Events

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 4

Options: 0 to 2147483647 events

Function: Together with the value of the Error Threshold parameter, establishes a criterion to evaluate the quality of the router/frame relay network connection. See the description of the Error Threshold parameter for more information.

Instructions: Enter the number of consecutive status exchanges you want the router to monitor.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.13

Parameter: Multicast

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables support for frame relay multicast service.

Instructions: Set to Enable if your frame relay subscription service provides multicast service, and if this frame relay interface should receive multicast messages.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.16

Parameter: Congestion Control

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: Disable

Options: Enable | Disable

Function: Enables or disables congestion control on this interface. If you set this parameter to Enable, the router drops all outbound traffic destined for a congested VC until the congestion clears. The value of this parameter affects all VCs that you do not individually configure.

Instructions: To activate congestion control, set to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.22

Parameter: Congestion Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the Congestion Counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared. The value of this parameter applies to all VCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.23

Parameter: Congestion Counter

Path: Configuration Manager > Protocols > Frame Relay > Interfaces

Default: 20

Options: 1 through 500 notifications

Function: Indicates the maximum number of congestion notifications that the router can receive during the congestion timer period before it stops transmitting. If the router reaches the value set by this parameter, it determines the line is congested and stops transmitting.

Instructions: Specify the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. The value of this parameter applies to all VCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.1.1.24

Parameter:	**Congestion Method**
Path:	Configuration Manager > Protocols > Frame Relay > Interfaces
Default:	Shutdown
Options:	Shutdown │ Throttle │ Throttle Then Shutdown
Function:	Specifies the method of congestion control: Shutdown -- terminates the VC when congestion occurs. Throttle -- queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled. Throttle Then Shutdown -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.
Instructions:	Select a setting appropriate to your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.1.1.37

SVC LAPF Parameters

If you configure SVCs, the LAPF values in the Frame Relay LAPF Parameters window (Figure A-3) are important to your network.

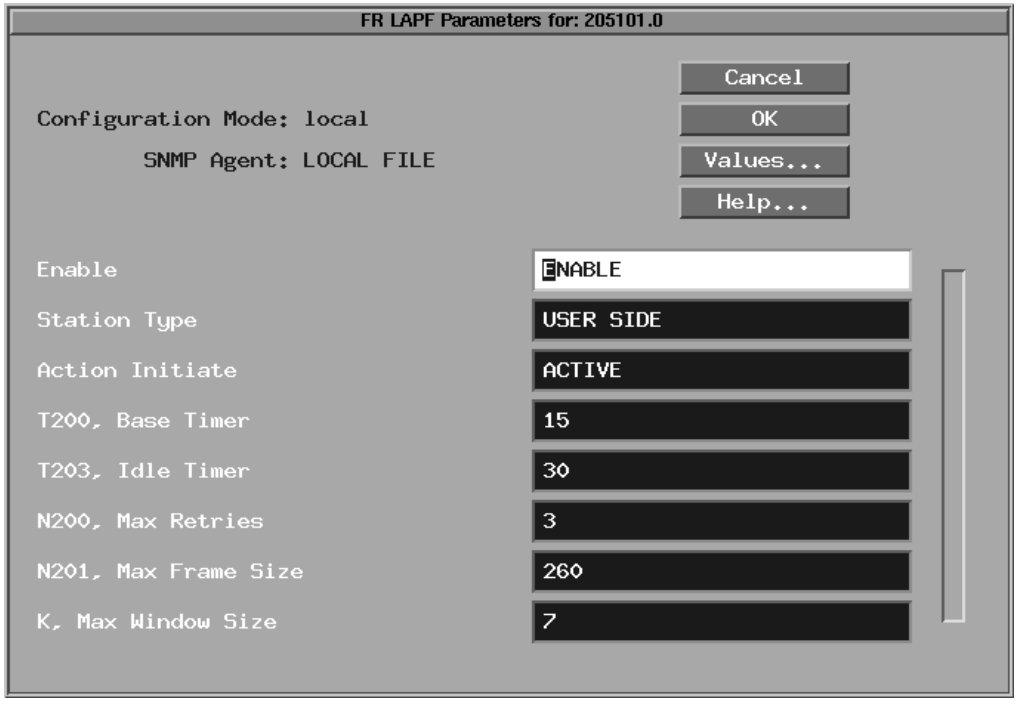

Figure A-3. FR LAPF Parameters Window

To access the FR LAPF Parameters window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Interfaces**.	The Frame Relay Interface List window opens.
4. Click on the **LAPF** button.	The Frame Relay LAPF Parameters window opens.

Parameter: Enable

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: Enable

Options: Enable │ Disable

Function: Enables or disables LAPF on this interface.

Instructions: To disable LAPF on this interface, set to Disable. Otherwise, accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.2

Parameter: Station Type

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: User Side

Options: Network Side │ User Side

Function: Identifies the desired station type of this interface.

Network Side indicates that LAPF will act as the data communications equipment.

User Side indicates that LAPF will act as the data terminal equipment.

Instructions: To have LAPF act as the DTE, accept the default, User Side. To have LAPF act as the DCE, set to Network Side.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.6

Parameter:	**Action Initiate**
Path:	Configuration Manager > Protocols > Interfaces > LAPF
Default:	Active
Options:	Active | Passive
Function:	Identifies the action LAPF will take to initiate link setup by sending or holding unnumbered command (SABME) frames to poll the router at the other end of the connection. Active indicates that LAPF will *send* SABME frames and initiate link setup. Passive indicates that LAPF will *hold* SABME frames and take no action to initiate link setup. To establish a LAPF link, at least one end of the connection has to initiate link setup.
Instructions:	To have LAPF initiate link setup from this router, accept the default, Active. To have LAPF take no action to initiate link setup, set to Passive.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.7.1.7

Parameter: **T200, Base Timer**

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: 15

Options: 1 to 1200 tenths of a second

Function: Indicates the amount of time (in tenths of a second) that the router waits to receive an acknowledgment from its remote peer.

This timer is the general purpose retransmission timeout. It is used during initiation of LAPF multiple frame support and for timeout of LAPF numbered information frames.

During initiation of LAPF multiple frame support, an unnumbered command (SABME) frame is sent to the peer LAPF to request multiple frame communications on the link. The peer LAPF responds with an unnumbered acknowledgment (UA) frame.

When multiple frame support has been established, numbered command/response information (I) frames are transmitted both ways across the connection. These I frames carry an acknowledgment of the highest number frame received by the sending LAPF.

In the event of a timeout, the sending platform retransmits the frame, up to the maximum number of times specified by the N200, Max Retries parameter.

Instructions: Set to the retransmission timeout value appropriate for your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.8

Parameter: **T203, Idle Timer**

Path: Configuration Manager > Protocols > Interfaces > LAPF

Default: 30

Options: 1 to 120 seconds

Function: Indicates the amount of time (in seconds) that the router allows for idle time with no data being transmitted. In the event of a timeout, the router initiates a frame handshake to check whether the connection is still up.

Instructions: Set to the idle time value appropriate for your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.9

Parameter: N200, Max Retries

Path: Configuration Manager > Protocols > Interfaces > LAPF
Default: 3
Options: 1 to 20
Function: Indicates the maximum number of LAPF retransmissions allowed on a connection after the T200 Base Timer expires before the connection terminates.
Instructions: Set to the value of retransmissions appropriate for your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.10

Parameter: N201, Max Frame Size

Path: Configuration Manager > Protocols > Interfaces > LAPF
Default: 260
Options: 260 to 2052 octets
Function: Indicates the maximum number of octets of data allowed in the LAPF information field. The larger the number allowed, the less overhead on the system. However, a large value could exceed the system buffer size. You should accept the default value.
Instructions: Set to the maximum size of the LAPF information field.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.11

Parameter: K, Max Window Size

Path: Configuration Manager > Protocols > Interfaces > LAPF
Default: 7
Options: 1 to 127
Function: Indicates the maximum number of outstanding numbered information (I) frames allowed across a connection. These are frames that have traveled across the link, but which the peer has not acknowledged. Each of these frames remains in a backup queue until the peer sends an acknowledge message. A longer queue adversely affects system performance. You should accept the default value.
Instructions: Set to the value appropriate for your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.7.1.12

SVC Signaling Parameters

If you configure SVCs, signaling parameters are important to your network. You can modify these parameters in the Frame Relay Signaling Parameters window (Figure A-4).

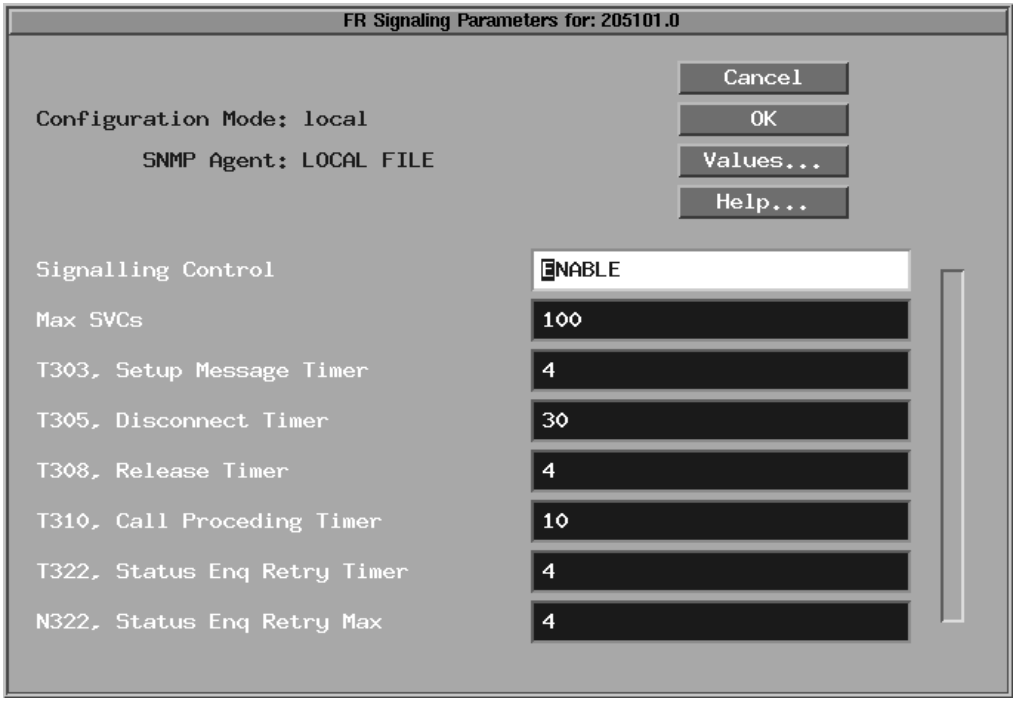

Figure A-4. Frame Relay Signaling Parameters Window

To access the Frame Relay Signaling Parameters window:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Choose **Interfaces**.	The Frame Relay Interface List window opens.
4. Click on the **Signaling** button.	The Frame Relay Signaling Parameters window opens.

Parameter: Signaling Control

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: Enable

Options: Enable │ Disable

Function: Enables or disables signaling on this interface.

Instructions: To use signaling on the interface, accept the default, Enable. If you do not want to use signaling, choose Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.2

Parameter: Max SVCs

Path: Configuration Manager > Protocols > Interfaces > Signaling

Default: 100

Options: 1 to 2147483647

Function: Indicates the maximum number of simultaneous switched virtual circuits allowed on the port. The more SVCs you allow on the port, the larger the system memory required to support them.

Instructions: Enter the maximum number of simultaneous SVCs per port for your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.5

Parameter: T303, Setup Message Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber.

In the event of a timeout, the router retransmits the setup message and restarts the timer. If the timer expires a second time, the call is cleared.

Instructions: Enter the timer value for call setup.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.6

Parameter: T305, Disconnect Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 30

Options: 20 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router sends a disconnect message and receives a release message back. This timer is used when this router initiates call clearing.

In the event of a timeout, the router sends a release message and enters the release request state. The timer is not restarted.

Instructions: Enter the timer value for call clearing.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.7

Parameter: T308, Release Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed for call clearing initiated by the other end of the connection or when the T305 Disconnect Timer expires:

- If timer T305 expires, the router enters the release request state, starts timer T308, and sends a release message.
- Timer T308 stops when the router receives a release complete message from the other end of the connection.

In the event of a timeout, the router retransmits the release message and restarts the timer. If the timer expires a second time, the call is cleared. The timer is not restarted.

Instructions: Enter the timer value for call clearing by the other end of the connection, or when timer T305 expires.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.8

Parameter: T310, Call Proceding Timer

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 10

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router receives a call proceeding message to the time the router receives a connect or disconnect message.

In the event of a timeout, the router clears the call. The timer is not restarted.

Instructions: Enter the timer value for call proceeding.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.9

Parameter: **T322, Status Enq Retry Timer**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 2 to 90 seconds

Function: Indicates the number of seconds allowed from the time the router sends a status inquiry message to the time the router receives an incoming status, disconnect, release, or release complete message.

If a timeout occurs, the router retransmits the status inquiry and restarts the timer. This occurs for the number of times set in the N322, Status Enq Retry Max parameter, after which the call will be cleared.

Instructions: Enter the timer value for status inquiries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.10

Parameter: **N322, Status Enq Retry Max**

Path: Configuration Manager > Protocols > Frame Relay > Interfaces > Signaling

Default: 4

Options: 1 to 20

Function: Indicates the maximum number of times the router will retransmit a status inquiry message.

If the router sends the maximum number of status inquiry messages and receives no response, the call is cleared.

Instructions: Enter a value for status inquiry retries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.9.1.11

Service Name Parameter

The Frame Relay Service List window (Figure A-5) contains the Service Name parameter, which identifies a service record.

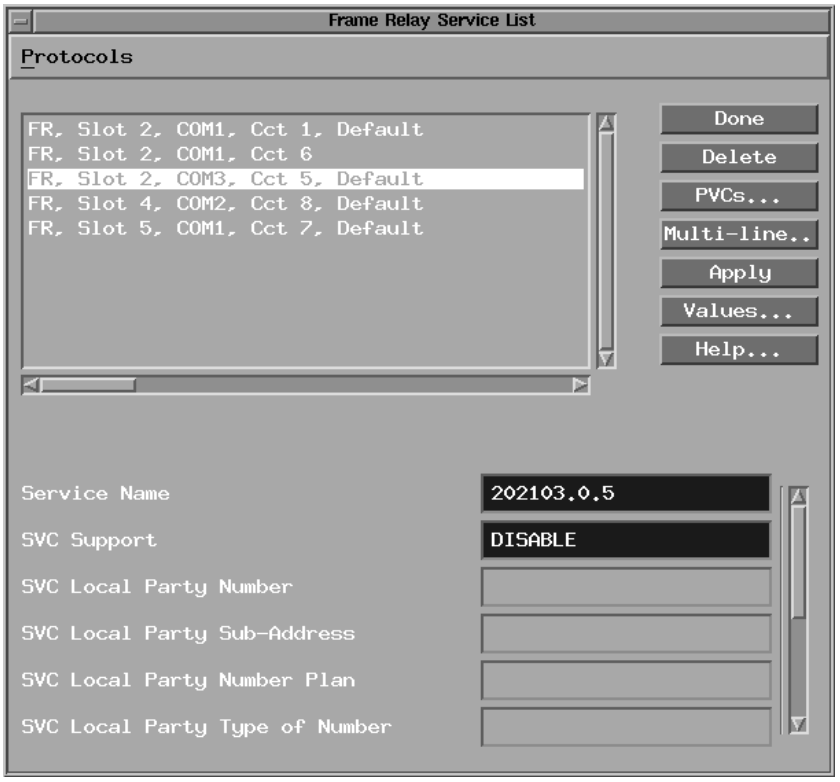

Figure A-5. Frame Relay Service List Window (for PVCs)

To access the Frame Relay Service List window:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

Parameter: Service Name

Path: Configuration Manager > Protocols > Frame Relay > Services

Default: None

Options: *<line_number>*.0.*<circuit_number>*

Function: Identifies the service record.

Instructions: Site Manager assigns a unique name in the given format. There is no need to change this value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.7

PVC Parameters

This section contains information about the following topics:

Topic	Page
DLCI Parameter for Each PVC	A-24
PVC Service Record Parameters	A-26
Multiline Algorithm Parameter	A-32

DLCI Parameter for Each PVC

The Frame Relay PVC Add window (Figure A-6) contains the DLCI Number parameter.

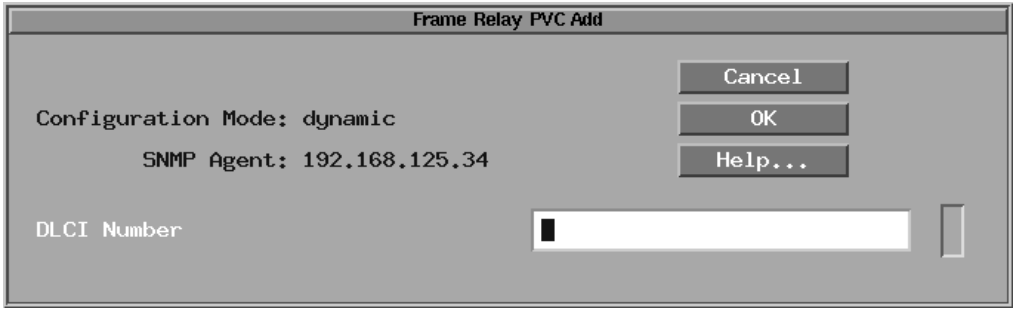

Figure A-6. Frame Relay PVC Add Window

To access the Frame Relay PVC Add window, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

(continued)

Site Manager Procedure	
You do this	**System responds**
4. Click on **PVCs**.	The FR PVC List for Service window opens.
5. Click on **Add**.	The Frame Relay PVC Add window opens.

Parameter: DLCI Number

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs > Add

Default: None

Options: The frame relay switch provider assigns DLCI numbers. These assigned numbers are valid options.

Valid DLCI numbers vary based on the frame relay address length. The DLCI numbers that the switch provider assigns are generally in the following ranges:

2 byte -- 16 to 1007
3 byte -- 1024 to 64511
4 byte -- 131072 to 4194303

Function: Specifies the PVC identification number that the frame relay network uses to direct data.

Instructions: Enter the decimal number that the frame relay provider assigns.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.4

PVC Service Record Parameters

The FR PVC List for Service window (Figure A-7) contains the PVC parameters. Initially, these parameters are set automatically when you add a PVC, but you can modify them.

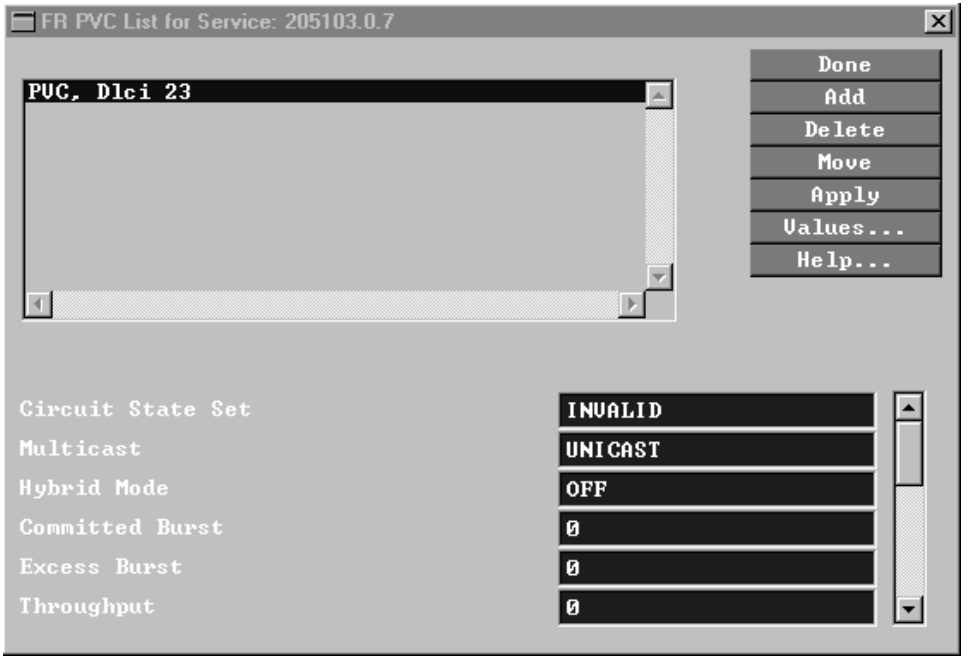

Figure A-7. FR PVC List for Service Window

To access the FR PVC List for Service window:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **PVCs**.	The FR PVC List for Service window opens.

Parameter: Circuit State Set

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Invalid

Options: Invalid │ Active │ Inactive

Function: Specifies the state of the PVC.

Instructions: To indicate to a frame relay switch that the PVC is available for use, set to Active. To indicate that the PVC is configured, but not available for use (for example, before your switch provider actually activates the PVC), set to Inactive. If the PVC is configured, but the switch is unaware of it, choose Invalid.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.7

Parameter: Multicast

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Unicast

Options: Unicast │ Multicast

Function: Indicates whether this PVC is multicast or unicast.

Instructions: Set to Unicast or Multicast according to PVC type, as the frame relay switch provider instructs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.19

Parameter: Hybrid Mode

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default: OFF
Options: ON | OFF
Function: Allows you to use the same PVC for both routing and bridging.
Instructions: If you do not want to enable both routing and bridging services, accept the default, OFF. If you do want to enable both routing and bridging, set to ON.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.1.2.1.24

Parameter: Committed Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default: 0
Options: 0 to 2147483647 bits
Function: The maximum number of bits that a VC can transmit during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, this parameter and the Throughput parameter (CIR) must both be greater than zero. The Committed Burst (Bc) value should be lower than the Throughput.
Instructions: Enter a value within the given range. You should set this parameter to 1/4 of the CIR unless this VC is sending frames larger than that size. If the VC is sending large frames, increase the value of this parameter to accommodate the size of those frames.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.16

Parameter: Excess Burst

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default: 0
Options: 0 to 2147483647 bits
Function: This value is added to the Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Excess Burst plus the Committed Burst must be less than or equal to the line speed.
Instructions: Enter a value within the given range.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.17

Parameter:	**Throughput**
Path:	Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default:	0
Options:	0 to 2147483647 b/s
Function:	The rate in bits per second at which data travels over this VC when no congestion is occurring. To enable traffic shaping, this parameter and the Committed Burst parameter must be set to values greater than zero.
Instructions:	Your carrier supplies the CIR or throughput value, which you enter in this parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.2.1.18

Parameter:	**Congestion Control**
Path:	Configuration Manager > Protocols > Frame Relay > Services > PVCs
Default:	Inherit
Options:	Disable | Enable | Inherit
Function:	Enables or disables congestion control on this interface.
Instructions:	To activate congestion control, set to Enable. This value tells the router to drop all traffic destined for a congested PVC until the congestion clears. To deactivate congestion control, set to Disable. If you want the Congestion Control setting for this PVC to match the setting you specify for the frame relay Interface Congestion Control parameter, accept the default, Inherit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.2.1.25

Parameter: Congestion Timer

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the Congestion Counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared.

If you set the Congestion Control parameter to Inherit, the PVC uses DLCMI for congestion control, not the value of this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.27

Parameter: Congestion Counter

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: 20

Options: 1 to 500 notifications

Function: Sets the maximum number of congestion notifications that the router can receive during the Congestion Timer period before it stops transmitting.

Instructions: Specify the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. Note, however, that if you set the Congestion Control parameter to Inherit, the PVC uses DLCMI for congestion control, not the value of this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.28

Parameter: Congestion Method

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Inherit

Options: Shutdown │ Throttle │ Throttle Then Shutdown │ Inherit

Function: Specifies the method of congestion control:

Inherit -- specifies that this VC will use the value of the interface Congestion Method parameter.

Shutdown -- terminates the VC when congestion occurs.

Throttle -- queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled.

Throttle Then Shutdown -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

Instructions: Choose a setting appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.33

Parameter: Compression Control

Path: Configuration Manager > Protocols > Frame Relay > Services > PVCs

Default: Enable

Options: Enable │ Disable

Function: Enables or disables data compression for this service record.

Instructions: To use data compression for this service record, accept the default, Enable. Otherwise, select Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.2.1.29

Multiline Algorithm Parameter

For each multiline configuration, you specify the multiline algorithm it should use. The Services Multilined With window (Figure A-8) contains the Multiline Algorithm to Choose Line parameter.

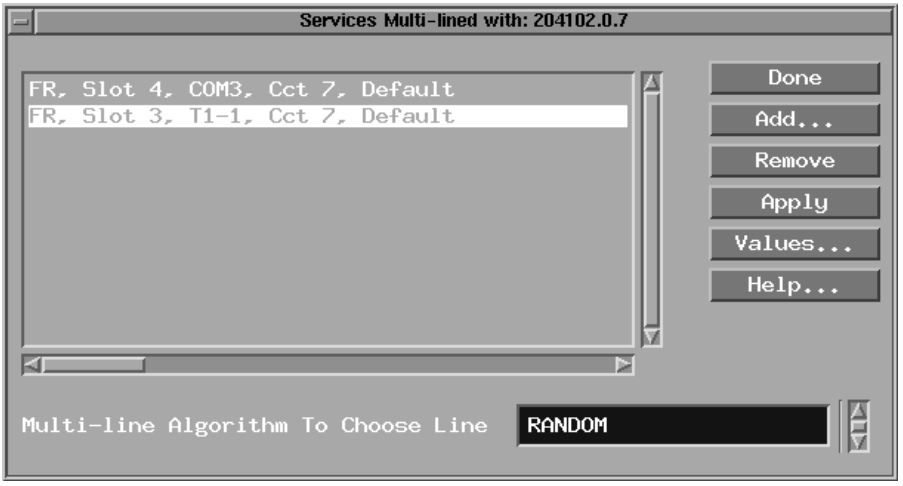

Figure A-8. Services Multilined With Window

To access the Services Multilined With window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager, choose **Protocols**.	The Protocols menu opens.
2. Choose **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on the **Multiline** button.	The Services Multilined With window opens.

This window lets you:

- Specify how a multiline circuit distributes traffic by setting the Multiline Algorithm to Choose Line parameter.
- Add multiline services to a circuit.

  Click on Add to open the Add Multiline Services window (Figure A-9). Next, click on a circuit entry and click on Select. When you do this, the circuit entry moves from the Add Multiline Services window to the Services Multilined With window, indicating that it has been added to the multiline circuit. The Add Multiline Services window closes.

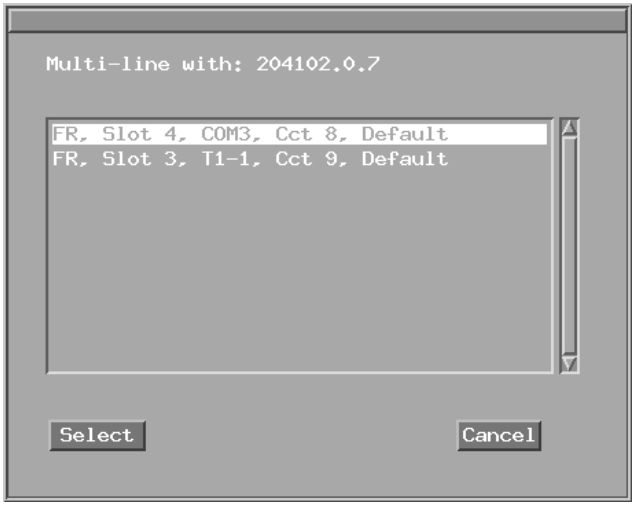

Figure A-9. Add Multiline Services Window

Parameter:	**Multiline Algorithm to Choose Line**
Path:	Configuration Manager > Protocols > Frame Relay > Services > Multiline
Default:	None
Options:	Random | Address Based
Function:	Specifies how the multiline circuit distributes traffic over its data paths, as follows: Random -- sends data alternately over the two paths. This method ensures even distribution among the lines, but the packets arrive out of sequence. Address Based -- sends data over the same data path if the traffic is going between the same source and destination address pair. This method ensures the data arrives in sequence.
Instructions:	Select an algorithm for the multiline circuits.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.1.1.23

C Service Record Parameters

This section contains the following information:

Topic	Page
SVC Service List Parameters	A-35
SVC Options Parameters	A-41
SVC Options List for Service Parameters	A-44

SVC Service List Parameters

The Frame Relay Service List window contains the SVC service list parameters (Figure A-10). These parameters apply to all of the SVCs in a service record, unless you configure SVCs individually with SVC Options parameters.

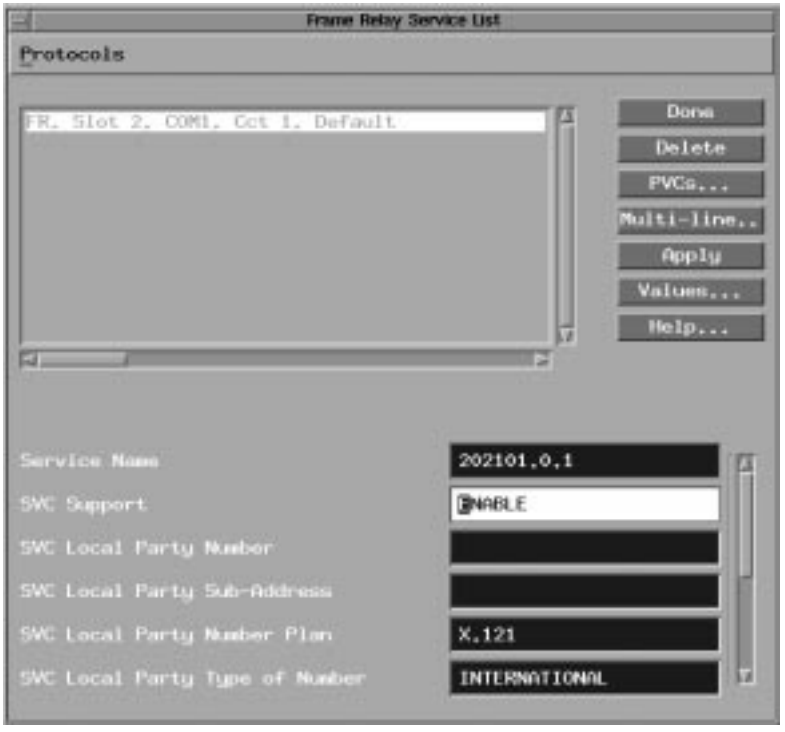

Figure A-10. Frame Relay Service List Window (for SVCs)

To access the Frame Relay Service List window:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.

You must enable the SVC Support parameter before you can modify the SVC parameters.

Parameter: Service Name

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: *<line_number>*.0.*<circuit_number>*
Function: Identifies the service record.
Instructions: Site Manager assigns a unique name in the given format. There is no need to change this value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.7

Parameter: SVC Support

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: Disable
Options: Enable │ Disable
Function: Enables or disables support for SVCs on this interface.
Instructions: If you want to configure SVCs on this interface, select Enable. Otherwise, accept the default, Disable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.17

Parameter: SVC Local Party Number

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: Any display string.
Function: Specifies the outbound calling party number, which is also the inbound called party number.
Instructions: Enter the number.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.18

Parameter: SVC Local Party Sub-Address

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: Any display string
Function: Specifies the outbound calling party subaddress, which is also the inbound called party subaddress.
Instructions: Enter the number.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.19

Parameter: SVC Local Party Number Plan

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: X.121
Options: E.164 | X.121
Function: Specifies whether this SVC uses the E.164 or X.121 number plan for addresses.
Instructions: Choose the numbering plan that applies to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.20

Parameter: SVC Local Party Type of Number

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: International
Options: Unknown | International
Function: Specifies the type of number the local caller uses.
Instructions: To allow the caller to use an international type number, accept the default, International. Otherwise, choose Unknown.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.21

Parameter: SVC Call Block

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: None
Options: None | Inbound | Outbound | All
Function: Allows you to block certain types of calls on the SVC.
Instructions: Choose the type of call blocking you want this SVC to use.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.22

Parameter: SVC InScreening Disable

Path: Configuration Manager > Protocols > Frame Relay > Services
Default: Disable
Options: Enable | Disable
Function: Allows you to screen incoming calls on this SVC.
Instructions: If you do not want to screen incoming calls, accept the default, Disable. To screen calls, choose Enable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.23

Parameter: **SVC InScreening Usage**

Path: Configuration Manager > Protocols > Frame Relay > Services

Default: Include

Options: Include | Exclude

Function: Enables you to allow or disallow calls from numbers in associated SVC option records.

Instructions: To allow these calls, accept the default, Include. Choose Exclude to disallow them.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.24

Parameter: **SVC Inactivity Timer**

Path: Configuration Manager > Protocols > Frame Relay > Services

Default: 60

Options: 0 to 2147483647 seconds

Function: Specifies the amount of time, in seconds, before the SVC terminates because no data has travelled over the circuit in the direction you specify in the Inactivity Mode parameter.

Instructions: If you want to set the timer to 1 minute, accept the default. Otherwise, specify another value within the allowable range.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.5.1.25

Parameter:	**SVC Inactivity Mode**
Path:	Configuration Manager > Protocols > Frame Relay > Services
Default:	Both Directions
Options:	Both Directions | Transmit Only | Receive Only | Either Direction
Function:	Specifies the direction of the data that the SVC Inactivity Timer monitors in determining whether to keep an SVC up or to terminate it. The options are: Transmit Only -- only data transmitted by the router prevents the expiration of the inactivity timer. If the router does not transmit any data, the inactivity timer expires and disconnects the SVC. Receive Only -- only data received by the router prevents the expiration of the inactivity timer. If the router does not receive any data, the inactivity timer expires and disconnects the SVC. Both Directions -- only data transmitted AND received by the router prevents the expiration of the inactivity timer. If the router does not transmit and receive data, the inactivity timer expires and disconnects the SVC. Either Direction -- only data transmitted OR received by the router prevents the expiration of the inactivity timer. If the router does not transmit or receive data, the inactivity timer expires and disconnects the SVC.
Instructions:	Select an option appropriate for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.5.1.26

SVC Options Parameters

You can edit SVC Options parameters in the Frame Relay SVC Options Add window (Figure A-11).

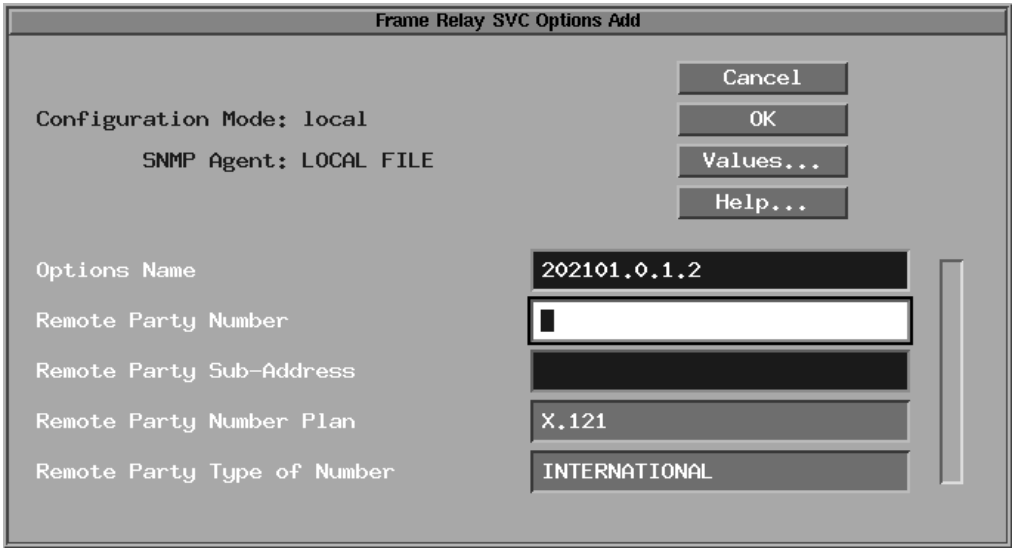

Figure A-11. Frame Relay SVC Options Add Window

To access the Frame Relay SVC Options Add window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **SVCs.**	The FR SVC Options List for Service window opens.
5. Click on **Add.**	The Frame Relay SVC Options Add window opens.

Parameter: Options Name

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs > Add

Default: None

Options: *<line_number>*.0.*<circuit_number>*

Function: Identifies the options record.

Instructions: Site Manager assigns a unique name in the given format. There is no need to change this value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.34

Parameter: Remote Party Number

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: None

Options: Any display string.

Function: Specifies the outbound called party number, which is also the inbound calling party number.

Instructions: Enter the number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.7

Parameter: Remote Party Sub-Address

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: None

Options: Any display string.

Function: Specifies the outbound called party subaddress, which is also the inbound calling party subaddress.

Instructions: Enter the number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.8

Parameter: Remote Party Number Plan

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: X.121

Options: E.164 | X.121

Function: Specifies whether the remote SVC uses the E.164 or X.121 number plan for addresses.

Instructions: Choose the numbering plan that applies to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.9

Parameter: Remote Party Type of Number

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: International

Options: Unknown | International

Function: Specifies the type of number the remote caller uses.

Instructions: If the caller uses an international type number, accept the default, International. Otherwise, choose Unknown.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.10

SVC Options List for Service Parameters

When you have finished editing the options parameters, you can return to the FR SVC Options List for Service window (Figure A-12) to edit the remaining options parameters.

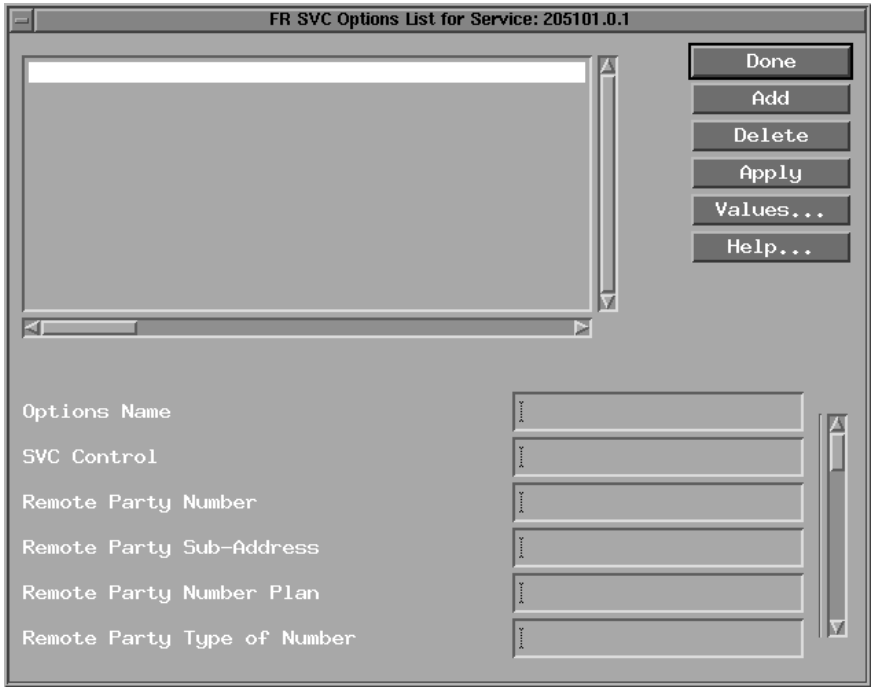

Figure A-12. FR SVC Options List for Service Window

To access the FR SVC Options List for Service window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. Click on the **Protocols** menu in the Configuration Manager menu bar.	The Protocols menu opens.
2. Click on **Frame Relay**.	The Frame Relay menu opens.
3. Click on **Services**.	The Frame Relay Service List window opens.
4. Click on **SVCs.**	The FR SVC Options List for Service window opens.

Parameter: SVC Control

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: Enable

Options: Enable │ Disable

Function: Enables or disables the SVC options record for this interface.

Instructions: To disable the SVC options record, select Disable. Otherwise, accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.2

Parameter: Broadcast Control

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: Enable

Options: Enable │ Disable

Function: Specifies whether the router includes this interface in outbound broadcasts.

Instructions: If you want this SVC to receive outbound broadcasts, accept the default, Enable. Otherwise, choose Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.11

Parameter:	**Inactivity Timer**
Path:	Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default:	60
Options:	0 to 2147483647 seconds
Function:	Amount of time, in seconds, before the SVC terminates because no data has traveled over the circuit in the direction you specify in the Inactivity Timer Mode parameter.
Instructions:	Accept the default, or set to a value appropriate for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.12

Parameter:	**Inactivity Timer Mode**
Path:	Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default:	Transmit Only
Options:	Transmit Only | Receive Only | Both Directions | Either Direction
Function:	Specifies the direction of the data that the SVC Inactivity Timer monitors to determine whether to keep an SVC up or to terminate it. The options are: Transmit Only -- only data transmitted by the router prevents the expiration of the inactivity timer. If the router does not transmit any data, the inactivity timer expires and disconnects the SVC. Receive Only -- only data received by the router prevents the expiration of the inactivity timer. If the router does not receive any data, the inactivity timer expires and disconnects the SVC. Both Directions -- only data transmitted AND received by the router prevents the expiration of the inactivity timer. If the router does not transmit and receive data, the inactivity timer expires and disconnects the SVC. Either Direction -- only data transmitted OR received by the router prevents the expiration of the inactivity timer. If the router does not transmit or receive data, the inactivity timer expires and disconnects the SVC.
Instructions:	Select an option appropriate for you network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.13

Parameter: X.213 Data Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the priority of data on the network connection as defined in ITU-T Q.933 and X.213. This is a value the router requests; it is not guaranteed. A value of 0 is the lowest priority, and 14 is the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.14

Parameter: X.213 Data LQA Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the lowest acceptable priority of data on a connection. A value of 0 is the lowest priority, and 14 is the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.15

Parameter: X.213 Gain Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the priority of data required to add a connection. This is a value that the router requests; it is not guaranteed. A value of 0 is the lowest priority, and 14 is the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.16

Parameter: X.213 Gain LQA Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the lowest acceptable priority of data to add a connection. This is a value below which the router will not create the SVC. A value of 0 is the lowest priority, and 14 is the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.17

Parameter: X.213 Keep Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the priority of data required to maintain a connection. This is a value that the router requests; it is not guaranteed. A value of 0 is the lowest priority, and 14 is the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.18

Parameter: X.213 Keep LQA Priority

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs

Default: 15

Options: 0 to 15

Function: Sets the lowest acceptable priority of data required to maintain a connection. This is a value below which the router will disconnect the SVC. A value of 0 is the lowest priority, and 14 is the highest. A value of 15 means unspecified.

Instructions: If your network supports X.213 prioritization, you should assign a value. You should accept the default if the network does not support X.213 prioritization, unless the network is able to accept pieces of signaling information that it does not recognize.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.19

Parameter: LL Core Out Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 0
Options: 0 to 21447463647 b/s
Function: Specifies the requested outgoing throughput (b/s) when no congestion is occurring. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions: Choose a value appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.20

Parameter: LL Core In Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 0
Options: 0 to 21447463647 b/s
Function: Specifies the requested incoming throughput (kbits/second) when no congestion is occurring. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions: Choose a value appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.21

Parameter: LL Core Min Out Throughput

Path: Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default: 0
Options: 0 to 21447463647 b/s
Function: Specifies the minimum acceptable outgoing throughput. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions: Choose a value appropriate to your network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.22

Parameter: LL Core Min In Throughput

Path:	Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default:	0
Options:	0 to 21447463647 b/s
Function:	Specifies the minimum acceptable incoming throughput. To enable traffic shaping, the throughput parameters and the burst parameters must be set to values greater than zero.
Instructions:	Choose a value appropriate to your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.23

Parameter: LL Core Out Committed Burst

Path:	Configuration Manager > Protocols > Frame Relay > Services > SVCs
Default:	0
Options:	0 to 21447463647 b/s
Function:	Specifies the outgoing committed burst size. This is the maximum number of bits that a VC can transmit during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, this parameter and the Throughput parameter (CIR) must both be greater than zero. The Core Out Committed Burst (Bc) value should be lower than the Core Out Throughput value.
Instructions:	Choose a value appropriate to your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.24

Parameter: LL Core In Committed Burst

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the incoming committed burst size. This is the maximum number of bits that a VC can receive during the VC's burst period (Tc) when congestion is occurring. To enable traffic shaping, the Burst parameters and the Throughput parameters (CIR) must be greater than zero. The Core In Committed Burst (Bc) value should be lower than the Core In Throughput value.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.25

Parameter: LL Core Out Excess Burst

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the outgoing excess burst size. This value is added to the Core Out Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Core Out Excess Burst plus the Core Out Committed Burst must be less than or equal to the line speed.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.26

Parameter: LL Core In Excess Burst

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 0

Options: 0 to 21447463647 b/s

Function: Specifies the incoming excess burst size. This value is added to the Core In Committed Burst value to determine the maximum number of bits that may be transmitted during the VC's burst period when there is no congestion. The Core In Excess Burst plus the Core In Committed Burst must be less than or equal to the line speed.

Instructions: Choose a value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.27

Parameter: Congestion Disable

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Inherit

Options: Enable | Disable | Inherit

Function: Specifies whether and how this SVC will use congestion control.

Inherit means that this SVC uses the value in the interface Congestion Control parameter.

Enable activates congestion control for this SVC regardless of the interface's parameter setting. If you enable congestion control, the router drops all outbound traffic from this SVC while congestion is occurring.

Disable means that the SVC will not use congestion control.

Instructions: Accept the default, or choose another value appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.28

Parameter: Congestion Timer

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 1

Options: 0.5 to 5 seconds, in 0.5-second intervals

Function: Specifies the length of time, in seconds, during which the router counts congestion notifications. If the router receives the number of congestion notifications set by the Congestion Counter parameter, the router stops transmitting data. The router resumes transmission once it stops receiving congestion notifications.

Instructions: Set the length of time the router should count congestion notifications from the network. If you set this parameter for a long time period, the router may be less likely to stop transmission for an intermittent congestion condition. However, the router may be slow to detect congestion, resulting in long transmission delays once the congestion has cleared.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.29

Parameter: Congestion Counter

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: 20

Options: 1 to 500 notifications

Function: Indicates the maximum number of congestion notifications that the router can receive during the congestion timer period before it stops transmitting. If the router reaches the value set by this parameter, it determines the line is congested and stops transmitting.

Instructions: Set the congestion count. The smaller the number, the more quickly the router detects congestion and stops transmitting. The value of this parameter applies to all VCs that you do not individually configure.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.30

Parameter: **Congestion Method**

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Inherit

Options: Shutdown │ Throttle │ Throttle Then Shutdown │ Inherit

Function: Specifies the method of congestion control:

Shutdown terminates the VC when congestion occurs.

Throttle queues traffic when congestion occurs; traffic resumes when congestion clears. This option is valid only when traffic shaping is enabled.

Throttle Then Shutdown first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. This option is valid only when traffic shaping is enabled.

Inherit uses the value in the Interface Congestion Method parameter.

Instructions: Choose a setting appropriate to your network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.31

Parameter: **Traffic Shaping Disable**

Path: Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add

Default: Disable

Options: Enable │ Disable

Function: Enables or disables traffic shaping on this SVC.

Instructions: Set this parameter as follows:

If you do not want to use traffic shaping on this SVC, accept the default, Disable, and do not set the LL Core parameters.

To use traffic shaping and accept the QoS the network provides, set this parameter to Enable, and do not configure the LL Core parameters.

To use traffic shaping, and negotiate QoS with the network, set this parameter to Enable, and also set the LL Core parameters.

To prevent the router from enforcing the CIR, accept the default, Disable, and also set the LL Core parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.9.10.1.32

Parameter:	**WCP Enable**
Path:	Configuration Manager (select a connector) > Edit Connector window > Edit Circuit > Services > Frame Relay Service List window > SVCs > Add
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables compression services for this SVC.
Instructions:	Accept the default, Enable, to use compression on this SVC. Choose Disable to disable but not delete compression services.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.9.10.1.33

Appendix B
RIP Management for Frame Relay SVCs

IP and IPX use RIP to inform network entities of routing topology changes. Both IP and IPX allow various controls over the frequency and destination of these packets. Because RIP packets can affect whether and how the router establishes and disconnects frame relay SVCs, these controls extend to frame relay SVCs. Table B-1 lists the IP, IPX, and frame relay configuration attributes that affect frame relay SVCs, and how they interact.

For more information about configuring RIP see *Configuring IP, ARP, RARP, RIP, and OSPF Services* and *Configuring IPX Services.*

Table B-1. RIP Parameters

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Both Directions	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	RIP packets will refresh the transmit inactivity timer; any connected SVCs will not disconnect due to inactivity.
Enabled	Disabled	Both Directions	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will not disconnect due to inactivity.
Enabled	Enabled	Both Directions	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	If no non-RIP packets are transmitted *and* no packets are received within the inactivity timer interval, the SVC disconnects.

(continued)

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Disabled	Both Directions	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	If no non-RIP packets are transmitted *and* no packets are received within the inactivity timer interval, the SVC disconnects.
Disabled	Enabled or Disabled	Both Directions	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are transmitted *and* no packets are received within the inactivity timer interval, the SVC disconnects.
Enabled	Enabled	Either Direction	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	RIP packets will refresh the transmit inactivity timer. If no packets are received within the inactivity timer interval, the SVC disconnects.
Enabled	Disabled	Either Direction	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	RIP packets will refresh the transmit inactivity timer. If no packets are received within the inactivity timer interval, the SVC disconnects.

(continued)

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Either Direction	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	If no non-RIP packets are transmitted *or* if no packets are received within the inactivity timer interval, the SVC disconnects.
Enabled	Disabled	Either Direction	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	If no non-RIP packets are transmitted *or* if no packets are received within the inactivity timer interval, the SVC disconnects.
Disabled	Enabled or Disabled	Either Direction	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are transmitted *or* no packets are received within the inactivity timer interval, the SVC disconnects.
Enabled	Enabled	Transmit	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will not disconnect due to inactivity.

(continued)

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Disabled	Transmit	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	RIP packets will refresh the transmit inactivity timer, any connected SVCs will not disconnect due to inactivity.
Enabled	Enabled	Transmit	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	If no non-RIP packets are transmitted within the inactivity timer interval, the SVC disconnects.
Enabled	Disabled	Transmit	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	If no non-RIP packets are transmitted within the inactivity timer interval, the SVC disconnects.
Disabled	Enabled or Disabled	Transmit	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are transmitted within the inactivity timer interval, the SVC disconnects.

(continued)

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Enabled	Receive	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	If no packets are received within the inactivity timer interval, the SVC disconnects.
Enabled	Disabled	Receive	Inactivity > RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	If no packets are received within the inactivity timer interval, the SVC disconnects.
Enabled	Enabled	Receive	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will connect to send RIP packets.	If no packets are received within the inactivity timer interval, the SVC disconnects.

(continued)

Table B-1. RIP Parameters *(continued)*

IP or IPX RIP Enable	IP or IPX RIP Frame Relay SVC Broadcast Enable	Frame Relay SVC Inactivity Timer Mode	Inactivity Timer, RIP Timer	RIP Timer Functionality	Inactivity Timer Functionality
Enabled	Disabled	Receive	Inactivity < RIP	When the RIP timer expires: • RIP packets will be sent over connected SVCs. • Any SVCs configured as adjacent hosts that are not connected will remain disconnected. SVCs will not connect and will not send RIP packets.	If no packets are received within the inactivity timer interval, the SVC disconnects.
Disabled	Enabled or Disabled	Receive	RIP timer not applicable, RIP is disabled.	Not applicable, RIP is disabled.	If no packets are received within the inactivity timer interval, the SVC disconnects.

Appendix C
Monitoring Frame Relay Using the BCC show Command

To display configuration and statistical data about frame relay, use the BCC **show** command.

This appendix includes descriptions of the following **show** commands:

Topic	Page
Online Help for show Commands	C-2
show frame-relay congestion	C-2
show frame-relay multiline	C-4
show frame-relay services	C-5
show frame-relay shaping	C-6
show frame-relay stats	C-7
show frame-relay summary	C-17
show frame-relay svcs	C-19
show frame-relay vcs	C-21

Online Help for show Commands

To display a list of command options, enter **show frame-relay ?** at any BCC prompt. To learn more about any **show frame-relay** command option and its syntax, use the question mark (**?**) command as follows:

```
bcc> show frame relay ?
  congestion      services        stats           svcs
  multiline       shaping         summary         vcs
bcc> show frame-relay svcs ?
  calls           priority        shaping
bcc> show frame-relay svcs calls?
show frame-relay svcs calls [-interface <arg>] [-service <arg>]
[-dlci <arg>]
```

show frame-relay congestion

Displays information about the congestion state and the configuration of frame relay VCs.

This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay VCs with the specified DLCI.
-interface *<name>*	Displays only frame relay VCs configured on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service.
-state {**forwarding | throttling | shutdown**}	Displays information about VCs in the following states: • *forwarding* -- shows only frame relay VCs that are forwarding. • *throttling* -- shows only frame relay VCs that are throttling. • *shutdown* -- shows only frame relay VCs that are shut down.

The output contains the following information:

Interface	Interface on which the frame relay circuit resides.
DLCI	Name of the VC associated with this circuit.
Enable	Status of congestion control: Disabled, Enabled, or Inherit. Inherit indicates that the VC should use the parameters from the DLCMI record.
State	Status of traffic; options are: • *forwarding* -- sending traffic at up to the maximum rate allowed on the PVC. • *congested* -- the PVC is not transmitting. • *throttling* -- the PVC is throttling back to the CIR rate.
Method	Identifies the congestion method: • *Shutdown* -- the VC terminates when congestion occurs. • *Throttle* -- the VC queues traffic when congestion occurs; traffic resumes when the congestion clears. • *Throttle then shutdown* -- first queues traffic when congestion occurs, and then terminates the VC if throttling does not alleviate congestion. • *Inherit* -- the VC uses the congestion method from the DLCMI record.
Timer	Length of time, in seconds, during which the router counts congestion notifications.
Counter	Maximum number of congestion notifications that the router can receive during the timer period before it stops transmitting.
Received FECN	Number of outbound forward explicit congestion notifications.
Received BECN	Number of outbound backward explicit congestion notifications.

show frame-relay multiline

Displays information about frame relay service information for multiline and shows PVCs that are priority information for active frame relay SVCs.

The **show frame-relay multiline** command supports the following subcommand options:

pvcs	services

In addition, you can specify the following command filters and filter arguments with the subcommand options:

-dlci *<dlci>*	Displays only VCs with the specified DLCI.
-name *<multiline_name>*	Displays only multiline PVCs or services on the specified frame relay multiline.

show frame-relay multiline pvcs

Displays PVCs that are priority information for active frame relay SVCs.

The output contains the following information:

Interface	Interface on which the frame relay SVC resides.
DLCI	Name of the SVC associated with this circuit.
Service-Name	Service name associated with the multiline.
Multiline-Name	Name of the multiline circuit.

show frame-relay multiline services

Shows frame relay information for multiline.

The output contains the following information:

Multiline-Name	Name of the multiline circuit.
Interface	Interface on which the multiline circuit resides.
Service-Name	Service name associated with the multiline.
Number of VCs	Total number of VCs on the multiline.

show frame-relay services

Displays general information about all frame relay services, including the number of VCs and SVC configurations. This command allows for the following command filters and filter arguments:

-interface *<name>*	Displays only frame relay services on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service record.

The output includes the following information:

Interface	Interface on which the frame relay circuit resides.
Service-Name	Unique name assigned to the service.
Total Number of VCs	Total number of VCs configured on this interface.
Number of VCs -- Static	Total number of static VCs configured on this interface.
Number of VCs -- Dynamic	Total number of PVCs dynamically learned.
Number of VCs -- SVCs	Total number of SVCs configured on this interface.
Number of VCs-- Active	Total number of VCs active on this interface.
Multiline	Specifies whether the service record is for multiline.

show frame-relay shaping

Displays information about the traffic shaping configuration of all frame relay VCs. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay VCs with the specified DLCI.
-interface *<name>*	Displays only frame relay VCs configured on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service.

The output includes the following information:

Interface	Interface on which the frame relay circuit resides.
DLCI	Name of the VC associated with this circuit.
CIR	Committed information rate.
Committed Burst	The maximum number of bits that the router can transmit over a specified time interval (B_c).
Excess Burst	The maximum number of extra bits the router attempts to send when there is no congestion (B_e).
Config Mode	Indicates whether the circuit is configured to use traffic shaping.
Congestion State	Status of traffic; options are: • *forwarding* -- sending traffic at up to the maximum rate allowed on the PVC. • *congested* -- the PVC is not transmitting. • *throttling* -- the PVC is throttling back to the CIR rate.

show frame-relay stats

The **show frame-relay stats** command displays statistical information about frame relay services.

The **show frame-relay stats** command supports the following subcommand options:

dlcmi	shaping
errors	signalling
lapf	vcs

show frame-relay stats dlcmi

Displays inbound and outbound statistics for frame relay DLCMIs. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only DLCMI interfaces configured on the specified interface.

The output contains the following information:

Interface	Interface on which the DLCMI resides.
Maximum Number of VCs	Number of DLCMIs associated with this circuit.
Current Number of VCs	Total number of DLCMIs configured on the router.
Sequence Counter	Next send sequence counter for DLCMI messages sent by the station.
Received Sequence	Send sequence number received in the last DLCMI message.
Passive Sequence	This station's send sequence for answering the DLCMI status enquiry message.
Passive Received	The sequence number received in the last DLCMI status enquiry message.

(continued)

Polls	Whether the station requests a full status report from the network or requests only a sequence number verification from the network.
Polls Missing	Number of missing status messages not received from a status enquiry.

show frame-relay stats error

Displays error statistics for frame relay interfaces. This command allows for the following command filter and filter argument:

-interface *<name>*	Displays only frame relay interfaces configured on the specified interface.

The output contains the following information:

Interface	Interface on which the frame relay SVC resides.
Last Error --Type	Type of the last error received.
Last Error -- Time	Time of the last error received.
Faults	Number of faults received.
Outbound Drops	Total number of outbound frames dropped because the SVC is inactive.
Inbound Discards	Total number of inbound frames discarded because they were deemed erroneous.

show frame-relay stats lapf

Displays LAPF receive, transmit, traffic, and error statistics for frame relay interfaces.

The **show frame-relay stats lapf** command supports the following subcommand options:

errors	traffic
receive	transmit

In addition, you can specify the following filter and filter argument with the subcommand options:

-interface *<name>*	Displays only frame relay VCs configured on the specified interface.

show frame-relay stats lapf errors

Displays LAPF error statistics for frame relay interfaces.

The output contains the following information:

Interface	Interface on which the VC resides.
Retransmission (T200 Timeouts)	Indicates the length of time the router waits to receive an acknowledgment from the station.
Idle (T203 Timeouts)	Indicates the amount of time that the router allows with no data being transmitted.
Retransmission Limit Exceeded (N200 Violation)	Indicates that the router sends the SABME message based on the value contained in the N200 counter (wfLapfN200) without receiving a reply.
Frame Size Exceeded (N201 Violations)	Number of information frames whose length exceeds the maximum number of octets defined by N201 (wfLapfN201).

show frame-relay stats lapf receive

Displays LAPF receive statistics for frame relay interfaces.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
Window	Number of outstanding signaling messages allowed.
SABME	Set Asynchronous Balanced Mode Extended (SABME): command that initiates multiple frame operation.
UA	Unnumbered acknowledgment (UA) is a response sent by a station upon receipt of a SABME or DISC command.
DISC	Disconnect (DISC) is a command that initiates the release of multiple frame operation.
DM	Disconnect mode (DM) indicates the collision of commands and responses that prevent the initiation of multiple frame operations.
FRMR	Frame Reject (FRMR) indicates errors encountered that cannot be recovered by resending an information frame.
REJ	Reject (REJ) requests retransmission of information frames.
RNR	Receive not ready (RNR) indicates that the station is temporarily busy and not ready to receive information frames.
RR	Receive ready (RR) indicates that the station is ready to receive information frames.
XID	Exchange ID indicates the station's identification information.

show frame-relay stats lapf traffic

Displays LAPF traffic statistics for frame relay interfaces.

The output contains the following information:

Interface	Interface on which the VC resides.
Unnumbered Frames Received	Number of frames received by LAPF in unnumbered format.
Numbered Frames Received	Number of frames received by LAPF.
Unnumbered Frames Sent	Number of frames sent by LAPF in unnumbered format.
Numbered Frames Sent	Number of frames sent by LAPF.

show frame-relay stats lapf transmit

Displays LAPF transmit statistics for frame relay interfaces.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
Window	Number of outstanding signaling messages allowed.
SABME	Set Asynchronous Balanced Mode Extended (SABME): command that initiates multiple frame operation.
UA	Unnumbered acknowledgment (UA) is a response sent by a station upon receipt of a SABME or DISC command.
DISC	Disconnect (DISC) is a command that initiates the release of multiple frame operation.
DM	Disconnect mode (DM) indicates the collision of commands and responses that prevent the initiation of multiple frame operations.
FRMR	Frame reject (FRMR) indicates errors encountered that cannot be recovered by resending an information frame.
REJ	Reject (REJ) requests retransmission of information frames.
RNR	Receive not ready (RNR) indicates that the station is temporarily busy and not ready to receive information frames.

(continued)

RR	Receive ready (RR) indicates that the station is ready to receive information frames.
XID	Exchange ID indicates the station's identification information.

show frame-relay stats shaping

Displays high queue, normal queue, low queue, and summary traffic shaping statistics for frame relay VCs.

The **show frame-relay stats shaping** command supports the following subcommand options:

high	normal
low	sum

In addition, you can specify the following command filters and filter arguments with the subcommand options:

-dlci *<dlci>*	Displays only VCs with the specified DLCI.
-interface *<name>*	Displays only VCs configured on the specified interface.
-service *<name>*	Displays only VCs on the specified service.

The syntax and information for the shaping subcommand options is as follows:

show frame-relay stats shaping high	Displays high queue outbound traffic shaping statistics for frame relay VCs.
show frame-relay stats shaping low	Displays low queue outbound traffic shaping statistics for frame relay VCs.
show frame-relay stats shaping normal	Displays normal queue outbound traffic shaping statistics for frame relay VCs.
show frame-relay stats shaping sum	Displays a summary of traffic shaping statistics for frame relay VCs.

The output for all the shaping subcommand options contains the following information:

Interface	Interface on which the frame relay VC resides.
DLCI	Name of the VC associated with this circuit.
Frames	Total number of frames that the router sends out this interface.
Inbound Drops	Total number of inbound frames dropped because the VC is inactive.
Frames Clipped from Queue	Number of high-, normal-, and low-priority clipped frames.
Maximum Frames in Queue	Maximum number of frames stored in the queue.
Queue Limit	Total number of buffers that the interface has to process frames.
Filter Dropped Frames	Total number of frames dropped because of congestion.
Large Frames	Number of large frames.

show frame-relay stats signalling

Displays receive and transmit statistics for frame relay interfaces.

The **show frame-relay stats signalling** command supports the following subcommand options:

receive	transmit

In addition, you can specify the following command filter and filter argument with the subcommand options:

-interface *<name>*	Displays only frame relay SVCs configured on the specified interface.

show frame-relay stats signalling receive

Displays signalling receive statistics for frame relay interfaces.

The output contains the following information:

Interface	Interface on which the SVC resides.
Setup	Indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber.
Call Proceeding	Message sent by the called subscriber to the router or by the router to the calling subscriber to indicate the establishment of the requested call.
Connect	Message sent by the called subscriber to the router and by the router to the calling subscriber to indicate call acceptance by the called subscriber.
Disconnect	Message sent by the subscriber to request the router to clear an end-to-end connection or a message sent by the router to indicate that the end-to-end connection is cleared.
Release	Message sent by the user or router to indicate that the sender has disconnected the call.
Release Complete	Message sent by the subscriber or the router to indicate that the sender has released the call reference.
Status	Message sent by the subscriber or router in response to a status enquiry or to report error conditions.
Unnumbered Frames Sent	Number of unnumbered acknowledgment frames (UAs) sent over SVCs to a subscriber or router.
Status Enquiry	Message sent by the subscriber or router to solicit a status message.

show frame-relay stats signalling transmit

Displays signalling transmit statistics for frame relay interfaces.

The output contains the following information:

Interface	Interface on which the frame relay SVC resides.
Setup	Indicates the number of seconds allowed from the time the router sends a setup message to the called subscriber and receives a connect or call proceeding message from the called subscriber.
Call Proceeding	Indicates the number of seconds allowed from the time the router receives a call proceeding message to the time the router receives a connect or disconnect message.
Connect	Message sent by the called user to the network and by the network to the calling user to indicate call acceptance by the called user.
Disconnect	Indicates the number of seconds allowed from the time the router sends a disconnect message and receives a release message back.
Release	Indicates the number of seconds allowed for a call clearing initiated by the other end of the connection or when the disconnect timer expires.
Release Complete	Indicates that the network returns a release complete message to the subscriber in response to a release message sent from the subscriber.
Status	Message sent by the user or network in response to a status enquiry or to report error conditions.
Unnumbered Frames Sent	Number of unnumbered acknowledgment frames (UAs) sent over SVCs to a subscriber or router.
Status Enquiry	Message sent by the user or network to solicit a status message.

show frame-relay stats vcs

Displays inbound and outbound statistics for frame relay VCs.

This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only VCs with the specified DLCI.
-interface *<name>*	Displays only VCs configured on the specified interface.
-service *<name>*	Displays only VCs on the specified service.
-type {**pvc | dynamic-pvc | svc**}	Displays information about only the type of VC configured: • *pvc* -- shows only statically configured PVCs. • *dynamic-pvc* -- shows only dynamically learned PVCs. • *svc* -- shows only SVCs.

The output contains the following information:

Interface	Interface on which the frame relay VC resides.
DLCI	PVC identification number that the frame relay network uses to direct data.
Inbound Frames	Total number of frames that the interface received.
Inbound Drops	Total number of outbound frames dropped because the VC is inactive.
Outbound Frames	Total number of frames that the router sent out on this interface.
Outbound Discard	Total number of frames dropped because the VC is inactive.
FECN	Number of outbound forward explicit congestion notifications.
BECN	Number of outbound backward explicit congestion notifications.

show frame-relay summary

Displays general information about all frame relay interfaces. You can display the current operational status and interface type.

This command allows for the following command filters and filter arguments:

-state {**enabled | disabled | error**}	Displays information about the state of the frame relay interfaces: • *enabled* -- shows only frame relay interfaces that are enabled. • *disabled* -- shows only frame relay interfaces that are disabled. • *error* -- shows only frame relay interfaces that are not present or are in a fault state.
-type {**backup | normal | primary | demand**}	Displays information about certain frame relay interface types: • *backup* -- shows only frame relay interfaces used to back up another frame relay interface. • *normal* -- shows only frame relay interfaces that are not backup, primary, or demand frame relay interfaces. • *primary* -- shows only frame relay interfaces that have a backup frame relay interface assigned to them. • *demand* -- shows only dial-on-demand frame relay interfaces.

The output includes the following information:

Interface	Interface on which the frame relay circuit resides.
Circuit	Name of the main frame relay circuit associated with this interface.
Management Type	Type of Data Link Control Management Interface (DLCMI) configured for the interface, as follows: • *Annex A* -- Management services as specified by ITU Annex A. • *Annex D* -- Management services as specified in Annex D to ANSI standard T1.617. • *Annex A Sw* -- Management services for the DCE side of the connection (Annex A). • *Annex D Sw* -- Management services for the DCE side of the connection (Annex D to T1.617). • *LMI* -- Management services as specified by Revision 1 of the Local Management Interface standard. • *LMI Sw* -- Management services for the DCE side of LMI. • *None* -- No management interface between the router and the frame relay network.
Interface Type	Interface type: Normal (leased service with no backup service), Primary/Shared (the backup circuit uses the primary configuration), Primary/Secondary (the backup circuit uses its own configuration).
Status	State of the interface as follows: • *Fault* -- Interface is not operating. • *Init* -- Interface is initializing (has not yet started). • *NotPres* -- Interface is not yet present. • *Running* -- Interface is operating properly.
Faults	Number of times the interface has been in fault mode.
Number of VCs -- Total	Total number of VCs configured on the interface.
Number of VCs -- Active	Total number of VCs active on the interface.
Services	Total number of frame relay service records or circuits.

show frame-relay svcs

Displays general information about all frame relay SVCs. You can display current operation status and SVC type.

The **show frame relay svcs** command supports the following subcommand options:

calls	shaping
priority	

In addition, you can specify the following command filters and filter arguments with the subcommand options:

-dlci *<dlci>*	Displays only frame relay SVCs with the specified DLCI.
-interface *<name>*	Displays only frame relay SVCs configured on the specified interface.
-service *<name>*	Displays only frame relay SVCs on the specified service record.

show frame-relay svcs calls

Displays call information for active frame relay SVCs.

The output contains the following information:

Interface	Interface on which the SVC resides.
DLCI	Name of the SVC associated with this circuit.
Direction	Direction of the call to the router: inbound or outbound.
Calling Number	Number the router is calling.
Called Number	Number of the router being called.

show frame-relay svcs priority

Displays priority information for active frame relay SVCs.

The output contains the following information:

Interface	Interface on which the SVC resides.
DLCI	Name of the SVC associated with this circuit.
Data Priority	Priority of data on the network connection. This is a value that the router requests; it is not guaranteed.
Gain Priority	Priority of data required to add a connection. This is a value that the route requests; it is not guaranteed.
Keep Priority	Priority of data required to maintain a connection. This is a value the router requests; it is not guaranteed.

show frame-relay svcs shaping

Displays shaping information for active SVCs.

The output contains the following information:

Interface	Interface on which the SVC resides.
DLCI	Name of the SVC associated with this circuit.
CIR	Committed information rate, or throughput, indicates the number of bits per second a carrier guarantees the router can transmit over a specified time period when there is no congestion.
Inbound Burst CIR	Number of requested incoming throughput (kbits/second) when there is no congestion.
Inbound Burst Committed	Number of bits that the router can receive over a specified time interval (B_c).
Inbound Burst Excess	Number of extra bits the router attempts to receive when there is no congestion (B_e).
Outbound Burst CIR	Requested outgoing throughput when no congestion is occurring.
Outbound Burst Committed	The number of bits that the router can send over a specified time interval (B_c).
Outbound Burst Excess	The number of extra bits the router attempts to send when there is no congestion (B_e).

show frame-relay vcs

Displays information about all those frame relay VCs with the specified DLCI. This command allows for the following command filters and filter arguments:

-dlci *<dlci>*	Displays only frame relay VCs with the specified DLCI.
-interface *<name>*	Displays only frame relay interfaces configured on the specified interface.
-service *<name>*	Displays only frame relay VCs on the specified service record.
-type {**pvc | dynamic-pvc | svc**}	Displays information about only those frame relay VCs of type: • *pvc* -- shows only statically configured PVCs. • *dynamic-pvc* -- shows only dynamically learned PVCs. • *svc* -- shows only SVCs.
-state {**active | inactive | invalid | xoff | control | starting**}	Displays information about only those VCs in one of the following states: • *active* -- VC is usable. • *inactive* -- VC is configured but not active. • *invalid* -- VC is configured but the switch has not confirmed it. • *xoff* -- VCs are XOFF'd. • *control* -- shows only control VCs. • *starting* -- shows VCs that are starting.

The output includes the following information:

Interface	Interface on which the frame relay circuit resides.
DLCI	Name of the virtual circuit associated with this interface.
State	State of the virtual circuit as follows: • *invalid* -- Circuit is configured but the switch has not confirmed it. • *active* -- Circuit is usable. • *inactive* -- Circuit is configured but not active. • *xoff* -- Specifies whether the router ignores or observes the XOFF bit in LMI. • *control* -- Circuit is a control VC. • *starting* -- Circuit is a starting VC.
Type	Type of circuit configured on the interface: • *pvc* -- PVC was statically configured. • *dynamic-pvc* -- PVC was dynamically learned. • *svc* -- VC is an SVC.
Hybrid	Indicates that you can use the same PVC for both routing and bridging.
Service	Service name associated with this PVC.

Index

A

access modes, description, 1-15
acronyms, xix
Action Initiate parameter, A-14
active state, 1-9
Address Length parameter, A-6
Address parameter, A-6
address resolution, for PVCs, 1-18
address-based distribution (multiline), 1-37
adjacent hosts, configuring for IP and IPX, 2-7
Annex A switch, 3-2
Annex D switch, 3-2

B

Bc
  configuring, for PVCs, 4-23
  configuring, for SVCs, 5-36
  description of, 1-24
BCC
  customizing, frame relay interfaces, 3-1
  customizing, PVCs, 4-1
  customizing, SVCs, 5-1
  show commands, C-1
  starting frame relay, 2-2
Be
  configuring, for PVCs, 4-23
  configuring, for SVCs, 5-36
  description, 1-24
BECN (backward explicit congestion notification)
  congestion control, 1-22
  definition of, 1-5
big pipe/little pipe topology, description, 1-19, 1-32
Broadcast Control parameter, A-45
buffers, for traffic shaping, 1-31

C

call blocking, configuring, 5-5
call present state, for LAPF, 1-12
call screening, configuring, 5-6
CIR
  configuration guidelines, 1-29
  configuring as 0, 1-24
  configuring, for PVCs, 4-24
  configuring, for SVCs, 5-37
  definition, 1-23
  enforcement, 1-24
  maximum value, 1-24
Circuit State Set parameter, A-27
Committed Burst parameter, A-28
committed burst rate. *See* Bc
committed information rate. *See* CIR
Compression Control parameter, A-31
compression. *See* data compression, 1-20
congestion control
  configuring, for PVCs, 4-15
  configuring, for SVCs, 5-26
  counters and timers for traffic shaping, 1-32
  description, 1-22
Congestion Control parameter, A-9, A-29
Congestion Counter parameter, A-10, A-30, A-54
Congestion Disable parameter, A-53
Congestion Method parameter, A-11, A-31, A-55
Congestion Timer parameter, A-10, A-30, A-54

conventions, text, xviii
customer support, xxii
customizing frame relay, 3-1, 4-1, 5-1

D

data clipping, for traffic shaping, 1-31
data compression, 5-40
  description, 1-20
  reenabling, for PVCs, 4-26
  with traffic shaping, 1-30
data link control identifier (DLCI), 1-5
default service record, 1-14
deleting
  frame relay service, 3-12
  PVCs, 4-7
  service records, for PVCs, 4-4
  service records, for SVCs, 5-4
dial services (backup and demand), for frame relay
  circuits, 1-38
direct mode, description, 1-16
disabling SVCs, 5-9
DLCI address length, selecting, 3-5
DLCI address type, selecting, 3-5
DLCI Number parameter, A-25
DLCMI (Data Link Control Management Interface)
  definition of, 1-7
  standards of, 1-7

E

Enable parameter (Interface), A-4
Enable parameter (SVC LAPF), A-13
enabling frame relay, 2-1
encryption, description, 1-21
Error Threshold parameter, A-8
error threshold, description, 3-8
Excess Burst parameter, A-28
excess burst. *See* Be
exchange identification (XID) frames, 1-9

F

FECN (forward explicit congestion notification)
  congestion control, 1-22
  definition of, 1-5
frame relay
  customizing interfaces, 3-1
  customizing PVCs, 4-1
  customizing SVCs, 5-1
  deleting from the router, 3-12
  overview, 1-2
  packet structure, 1-5
  RIP management, for SVCs, B-1
  show commands, for BCC, C-1
  starting, 2-1
Full Enquiry Interval parameter, A-7
full enquiry interval, description, 3-8

G

group mode, description, 1-15

H

header format
  2-byte, 1-6
  3- or 4-byte, 1-6
high queue limit, configuring, 4-22
hybrid mode
  configuring, 4-12
  description, 1-16
Hybrid Mode parameter, A-28

I

Inactivity Timer Mode parameter, A-46
Inactivity Timer parameter, A-46
inactivity timing (SVCs)
  configuring, 5-25
  overview, 1-33
interface parameters, A-2
IP adjacent hosts, cofiguring, 2-7
IPX adjacent hosts, configuring, 2-7

K

K, Max Window Size parameter, A-16

L

LAPF
- active state, 1-9
- call present state, 1-12
- call proceeding processing, 1-13
- call setup processing, 1-11
- categories of management frames, 1-9
- connect message processing, 1-13
- description of, 1-8
- disconnect message processing, 1-13
- exchange identification (XID) frames, 1-9
- incoming call proceeding, 1-12
- N200 retransmission timeout, 1-10
- numbered supervisory frames, 1-9
- operational states, 1-9
- parameters, modifying, 5-11
- release message processing, 1-14
- release request state, 1-12
- retransmission timeouts, 1-10
- retransmission timer, 1-10
- setup processing, 1-13
- SVC signaling, 1-8, 1-11
- T200 retransmission timeout, 1-10
- T203 retransmission timeout, 1-11
- TEI-assigned state, 1-9
- timeout timer, 1-9, 1-10
- timer recovery state, 1-9
- unnumbered control frames, 1-9

link management
- call present state, 1-12
- call proceeding processing, 1-13
- call setup processing, 1-11, 1-13
- categories of LAPF management frames, 1-9
- connect message processing, 1-13
- disconnect message, 1-13
- exchange identification (XID) frames, 1-9
- incoming call proceeding, 1-12
- LAPF operational states, 1-9
- LAPF timeout and retransmission timers, 1-9, 1-10
- numbered information frames, 1-9
- numbered supervisor frames, 1-9
- release message, 1-14
- release request state, 1-12
- SVC signaling, 1-8, 1-11
- timers, 1-12
- unnumbered control frames, 1-9

LL Core In Committed Burst parameter, A-52

LL Core In Excess Burst parameter, A-53

LL Core In Throughput parameter, A-50

LL Core Min In Throughput parameter, A-51

LL Core Min Out Throughput parameter, A-50

LL Core Out Committed Burst parameter, A-51

LL Core Out Excess Burst parameter, A-52

LL Core Out Throughput parameter, A-50

LMI (Local Management Interface), 1-7, 3-2, A-5

low queue limit, configuring, 4-22

M

management protocols. *See* DLCMI

management type, selecting, 3-2

Max SVCs parameter, A-18

Mgmnt Type parameter, A-5

Monitored Events parameter, A-8

moving PVCs, 4-9

MTU size for frame relay connections, 1-39

Multicast parameter, A-9, A-27

multicast, enabling, 4-10

multiline
- configuring, 4-27
- description of, 1-35
- removing, 4-28
- traffic distribution over lines, 1-36

Multiline Algorithm to Choose Line parameter, A-34

N

N200 retransmission timeout, 1-10
N200, Max Retries parameter, A-16
N201, Max Frame Size parameter, A-16
N322, Status Enq Retry Max parameter, A-21
network congestion, 1-22
normal queue limit, configuring, 4-22
numbered information frames, 1-9
numbered supervisory frames, 1-9

O

Options Name parameter, A-42
oversubscribing the interface, traffic shaping, 1-31
overview of frame relay, 1-2

P

packet structure, frame relay, 1-5
pass-through. *See* PVC pass-through
Polling Interval parameter, A-7
polling interval, description, 3-7
product support, xxii
protocol prioritization
  and multiline, 1-37
  definition of, 1-21
  with traffic shaping, 1-25
publications, hard copy, xxi
PVC pass-through
  configuring, 4-13
  overview, 1-37
PVCs
  adding to a service record, 1-15, 4-5
  configuring a default service record, 2-4
  deleting, 4-7
  description, 1-3
  moving, 1-15, 4-9
  parameters, A-24

Q

QoS (Quality of Service), 1-25
  customizing for SVCs, 1-28, 5-35

R

random traffic distribution (multiline), 1-36
release request state, for LAPF, 1-12
Remote Party Number parameter, A-42
Remote Party Number Plan parameter, A-43
Remote Party Sub-Address parameter, A-42
Remote Party Type of Number parameter, A-43
retransmission timeouts, 1-10, 1-11
RFC 1490, 1-18
RIP, and SVCs, 1-34, B-1

S

Service Name parameter, A-23, A-36
service records
  adding, 4-3, 5-2
  default service record, 1-14
  deleting, 3-12, 4-5, 5-4
  grouping for multiline, 4-27
  multiple, for an interface, 1-15
  overview, 1-14
  parameters, for PVCs, A-26
  parameters, for SVCs, A-35
show commands, BCC, C-1
signaling
  call proceeding processing, 1-13
  call setup processing, 1-11, 1-13
  connect message processing, 1-13
  for SVCs, 1-11
  parameters, modifying, 5-17
Signalling Control parameter, A-18
Site Manager
  customizing, frame relay interfaces, 3-1
  customizing, PVCs, 4-1
  customizing, SVCs, 5-1
  parameters, A-1
  starting frame relay, 2-3

source routing using RFC 1490, 1-18
starting frame relay, 2-1
Station Type parameter, A-13
support, Nortel Networks, xxii
SVC Call Block parameter, A-38
SVC Control parameter, A-45
SVC Inactivity Mode parameter, A-40
SVC Inactivity Timer parameter, A-39
SVC InScreening Disable parameter, A-38
SVC InScreening Usage parameter, A-39
SVC Local Party Number parameter, A-37
SVC Local Party Number Plan parameter, A-37
SVC Local Party Sub-Address parameter, A-37
SVC Local Party Type of Number parameter, A-38
SVC screen control, configuring, 5-6
SVC screen usage, configuring, 5-6
SVC Support parameter, A-36
SVCs, 1-12
  adding options to service records, 5-7
  call proceeding message, 1-13
  call proceeding processing, 1-13
  call setup processing, 1-11, 1-13
  categories of management frames, 1-9
  configuring a default service record, 2-6
  connect message, 1-13
  connect message processing, 1-13
  definition, 1-3
  disabling, 5-9
  disconnect message, 1-13
  disconnect message processing, 1-13
  disconnecting active circuits, 5-10
  exchange identification (XID) frames, 1-9
  frame relay signaling, 1-8
  incoming call proceeding, 1-12
  LAPF and signaling, 1-8
  LAPF operational states, 1-9
  LAPF signaling, modifying, 5-11
  LAPF timeout and retransmission timers, 1-10
  N200 retransmission timeout, 1-10
  numbered information frames, 1-9
  numbered supervisory frames, 1-9
  parameters, LAPF, A-12
  parameters, service records, A-35
  parameters, signaling, A-17
  release message processing, 1-14
  release request state, 1-12
  retransmission timeouts, 1-10, 1-11
  RIP management configuration, B-1
  setup message, 1-11, 1-13
  signaling, 1-11
  T200 retransmission timeout, 1-10
  unnumbered control frames, 1-9
synchronous line configuration, for frame relay circuits, 1-38

T

T200 retransmission timeout, 1-10
T200, Base Timer parameter, A-15
T203, Idle Timer parameter, A-15
T303, Setup Message Timer parameter, A-19
T305, Disconnect Timer parameter, A-19
T308, Release Timer parameter, A-20
T310, Call Proceding Timer parameter, A-20
T322, Status Enq Retry Timer parameter, A-21
technical publications, xxi
technical support, xxii
Technician Interface, configuring buffers for traffic shaping, 1-31
TEI-assigned state, 1-9
text conventions, xviii
throttling
  as a congestion method, A-11
  description, 1-24
Throughput parameter, A-29
timer recovery state, 1-9
timers
  for call setup, 1-12
  for LAPF, 1-10
  retransmission, 1-10, 1-11
traffic control, big pipe/little pipe topology, 1-19, 1-32
traffic distribution for multiline, 1-36

traffic shaping
buffer queue limits, 1-31
CIR, description, 1-23
committed burst rate, 1-24
configuration guidelines, 1-29
customizing, for PVCs, 4-21
customizing, for SVCs, 5-33
data clipping, 1-31
description, 1-23
excess burst rate, 1-24
for SVCs, 1-27
monitoring statistics, 1-30
oversubscribing the interface, 1-31
quality of service
description, 1-25
PVCs, 1-25
SVCs, 1-27
with data compression, 1-30
Traffic Shaping Disable parameter, A-55

U

unnumbered control frames, for LAPF, 1-9

V

virtual circuits, description, 1-2

W

WCP Enable parameter, A-56

X

X.213 Data LQA Priority parameter, A-47
X.213 Data Priority parameter, A-47
X.213 Gain LQA Priority parameter, A-48
X.213 Gain Priority parameter, A-48
X.213 Keep LQA Priority parameter, A-49
X.213 Keep Priority parameter, A-49
X.213 priority
configuring, 5-41
description, 1-33
XOFF bit, configuring, 3-4